面向21世纪本科生教材

抽象代数

牛凤文 编著



全国优秀出版社
武汉大学出版社

面向21世纪本科生教材

责任编辑：顾素萍

封面设计：涂　驰



ISBN 7-307-01229-4/O·101
定价：23.00元

面向21世纪本科生教材

抽象代数

牛凤文 编著







全国优秀出版社
武汉大学出版社

图书在版编目(CIP)数据

抽象代数/牛凤文编著. —武汉：武汉大学出版社，1992.4
面向21世纪本科生教材
ISBN 7-307-01229-4
Ⅰ.抽… Ⅱ.牛… Ⅲ.高等数学:抽象代数 Ⅳ.O182.2

责任编辑：顾素萍　　责任校对：杜　强　　版式设计：支　笛

出版发行：**武汉大学出版社**　(430072　武昌　珞珈山)
(电子邮件：wdp4@whu.edu.cn　网址：www.wdp.whu.edu.cn)
印刷：湖北民政印刷厂
开本：850×1168　1/32　印张：15.75　字数：403千字
版次：1992年4月第1版　　2003年10月第4次印刷
ISBN 7-307-01229-4/O·101　　定价：23.00元

内 容 提 要

本书系统地介绍抽象代数学的基本概念和基础知识，共七章。主要内容有群、群同态与商群；环、环同态与商环；域与域的扩张。

本书叙述深人浅出，文字生动活泼，例题充实新颖有典型性，推理自然详尽，重点突出而难点分散，可供综合性大学或师范院校数学专业作为教材，亦可供从事初等数学教学和研究工作的教师学习参考，也可以作为计算机科学、物理学、生物学和化学有关领域的工作人员的代数学普及读物。

前　言

（一）

古典代数学以研究代数方程的求解为中心，其历史源远流长．

19世纪初，年青数学家伽罗华（Galois）应用群的概念对高次代数方程是否可用根式求解问题进行了透彻研究并给出了明确回答．他成为抽象代数学新思想的启蒙者．

随后，这种把代数学变成集合论的、公理化的科学的改造不断强化，产生了很多新的思想、新的方法、新的观点和新的结果．

到了20世纪20年代，数学的最古老的分支之一的代数学完成了一次根本性的革命．它的标志是范德瓦尔登（Van der Waerden）的《近世代数学》一书的出版．

时至今日，抽象代数学已经成为很多数学分支中最常用的工具，空前普及，以至近年来，人们不再把这门学问冠之以“近世”、“抽象”等高贵头衔，而朴素地称它为《一般代数学》、《基础代数》，甚至《代数学》．

我们把这本书仍然称为《抽象代数学》只是想把它与仅仅讨论以数为对象的那种经典代数学加以区别．

抽象代数学是古典代数学发展的质的飞跃．学好本课程，可以对初等数学中很多容易模糊含混的问题，如算律、逆运算、多项式与根、因式分解等在公理系统中得以明确．

要在高观点之下认识初等代数，学习些抽象代数知识是绝对必要的．

近年来，抽象代数学本身仍在不断地发展．一方面，它在实际应用中找到了用武之地，如群论在晶体对称、运动和生物学中的应用，群论在研究物质结构模型中的应用，布尔代数、泛代数和代数编码在数理逻辑和计算机科学中的应用．另一方面，代数学向数学内部各相邻分支扩展、渗透，使同调代数、李群与李代数、微分代数、范畴论、半群理论与模论等成为学习拓扑学、泛函分析、微分方程论等必不可少的现代准备知识．

人们要在现代数学的学习和研究中有所发展，也需要学习些抽象代数学知识和思想方法．

因此，本书可以作为从事初等数学教学和研究工作的同志的提高书；可以作为要进一步学习代数学、泛函分析、拓扑学和微分方程论的同志的代数入门书；它也可以作为工作在计算机科学、物理学、生物学和化学有关领域的同志的代数学普及读物．

（二）

抽象代数学是数学中最适合于自学的学科之一．笔者就接触过大批自学抽象代数学取得成功的中学数学教师、科技工作者，很多人并没有在课堂上学过抽象代数课程，经过自学钻研，现在却在讲坛上自如地讲授“群论在物理中的应用”、“群论在化学中的应用”、“工程师用的代数学”，等等．

本课程只假定读者学过中学代数并知道一点矩阵运算规则，此外不要求任何高等数学内容做为准备知识．当然，学过解析几何和高等代数的读者理解本课程的概念会快些，但没学过这类课程的同志直接攻读抽象代数学，一般来说，应该没有原则性障碍．

学好本课程的关键在于对“公理化方法”实质和一些重要抽象概念的理解．

初学者往往被代数学中一个接一个的新概念所困扰，难理解又容易忘记．这实际上是理解的深刻程度的问题，只要读者对重要概念多花些工夫、多思考、多琢磨、多分析比较各种实例，最后能达

到用自己的习惯语言描述这些概念,逐渐就能运用自如.

整个课本中,抽象概念很多.但真正重要的、具有开创意义的,不过3、5个而已.只要把这几个概念理解透彻,对于其余属平行引进性质的东西就不需每个都花费同样大的气力了.

切忌把抽象代数学单纯作为"知识"来学,平均使用力量,每个定义都能背下来,但没有一个能"悟出真谛".学习抽象代数学的一个重要目的是提高"抽象思维"能力.

(三)

本书共分七章.第二章和第三章为群论初步,第四章介绍环论,第七章讨论域的扩张理论.其余三章是准备或过渡或处理专门问题的.

第二章和第三章在本书中地位显要.它给出了处理一个代数体系的"全过程".对于初学者来说,每个想法,每个解决办法都是新的.所说的初等代数到近世代数的"飞跃",即从研究数的运算到研究抽象代数系统的结构之"飞跃",就在这里完成.

处理其他代数系统的问题,虽然各有各的特点和侧重面,但群论中的思想方法对所有代数体系的研究都有指导意义.

关于本书中主要概念的重要程度、中心内容的依赖关系、对读者科学地分配学时的建议可分别见附表1和目录.

(四)

现将本书编写过程中的一些想法和做法说明一下.

(1) 课程的具体内容分为四级,最重要的结果称为定理,次之者称为命题,为配合理解定义、定理和命题而举的例是经过选择而有代表意义的,读者应弄懂它们所能说明的问题.每节所穿插的例题不要求读者一定记住.通常,例题中所用的解题方法属典型技巧而且思路比较明确,值得借鉴.

(2) 书中使用了不很明确的语言,分别加上了引号,如"拼

凑"、"缩影"等，读者能大致体会出意思就可以了.

(3) 在定理和命题的证明中有时夹杂着一些猜测和分析性的语言，这样易于理解证明的思路，但不太整齐规范.有时在证明之前把分析想法单列出来，证明就显得干净利落些，读者做习题时应采取后面的办法，分析部分可以不写出来.

(4) 在定理和命题的证明中，如果多说几句话就可直接证明的事情，一般就不一定引用前面某章某节某定理，因为许多读者时间分散，学后面内容时对前面很久以前读过的内容可能已有些遗忘，要求不断地翻回去重看，思想上会产生压力.

(5) 对于抽象代数学中最重要的概念和思想方法，采取难点分散、逐渐加深理解的方法，每次遇到都认真对待.如，等价关系、商集、陪集、商群、剩余环这一个系列；又如，子集生成的子群、子环、理想、子域这一个系列，等等.

(6) 凡是没有列入书后索引的术语，读者可按各种汉语词典的解释加以理解，如"组成"、"充分必要条件"、"蕴涵"、"程序"，等等.

(7) 每节所附的习题并不是按难易程度决定其前后顺序.前面的习题没做出来时，可以放一放，经过一段时间学习与复习后再做，对读者仍然有好处.

面向21世纪本科生教材

高等数学教程（上、下册）

空间解析几何

☞ 抽象代数

复变函数

线性空间引论

常微分方程

泛函分析基础

数学物理方程

计算方法

信息论基础

数值计算方法

离散数学

运筹学及其应用

线性规划

目　　录

第一章　集合、映射和关系

本课程要对多种多样的代数体系进行分析、比较、归纳、概括，从理论上加以抽象化、公理化，背景十分广泛．笼统说来，代数体系是一些有代数运算的集合．所以，我们首先要熟悉集合论中的基本概念、符号和思维方法．

这一章是抽象代数学的基础，也差不多是所有现代数学分支的基础．

为使自学者不过多依赖其他参考书，使本书基本上自成体系，这里可以说是从头讲起．

对集合和映射概念比较熟悉的读者可对照例题检查一下自己原有的理解是否正确．初学者则必须认真地弄懂定义中每一个字的含义，搞清楚定理证明和习题中每一步推理的根据．

第三节中，等价关系与分类、商集与自然映射都是本书中经常用到的，而且要不断深化的概念，读者必须很好地掌握．

§1　集　　合

在中学阶段，大家已经反复使用诸如集合、元素等概念．每一组对象的全体形成一个**集合**，集合里的各个对象叫做这个集合的**元素**．

本书用大写英文字母 $A,B,C,\cdots$ 代表集合，用小写英文字母 $a,b,c,\cdots$ 表示元素．

例如，这里有某青年小组名单如下

张奋学,22 岁,男,拟考抽象代数学;

王忠,26 岁,男,拟考英语;

李立,22 岁,女,拟考政治经济学;

张自强,29 岁,男,拟考英语;

王群,22 岁,女,拟考英语.

那么,本组王姓青年的集合是

$$\{王忠,王群\};$$

该组人员年龄组成的集合是

$$\{22 岁,29 岁,26 岁\};$$

他们中男青年拟考课程的集合为

$$\{抽象代数学,英语\}.$$

用 **I** 代表所有整数形成的集合;用 **R** 代表所有实数形成的集合;用 **C** 代表所有复数形成的集合.

$a\in A$ 表示 a 是集合 A 的一个元素,也说是 a 属于 A, A 含有 a. 如果 a 不是 A 的元素,则记为 $a\notin A$,也说是 a 不在 A 里,A 不含 a.

定义 1 集合 A 和 B 是**相等**的(记为 $A=B$)当且仅当 A 的每个元素都是 B 的元素且 B 的每个元素都是 A 的元素.

由此定义知道,如果要列举出一个集合的所有元素,那么列举的顺序是无关紧要的. 例如

$$\{22 岁,29 岁,26 岁\}=\{29 岁,26 岁,22 岁\},$$

$$\{春,夏,秋,冬\}=\{秋,春,冬,夏\}.$$

在一个无穷集合中列举其元素的方法更可用很多不同方式,例如

$$\begin{aligned}&\{2,4,6,\cdots,1,2,3,\cdots\}\\&=\{\cdots,6,4,2,1,3,5,\cdots\}\\&=\{1,2,3,4,\cdots\}.\end{aligned}$$

今后,我们最常用的确定一个集合的方法是所谓**描述方法**,即用数学表达式给出该集合元素的性质. 例如,整数 72 的所有因数的集合

$\{\pm 72, \pm 36, \pm 18, \pm 24, \pm 12, \pm 6, \pm 4, \pm 3, \pm 2, \pm 1, \pm 8, \pm 9\}$
可记为

$$\{a \in \mathbf{I} \mid a \text{ 整除 } 72\};$$

对于取定坐标系的平面 $\mathbf{R}_2$ 上以原点为中心的单位圆上所有点所形成的集合可记为

$$\{(x, y) \in \mathbf{R}_2 \mid x^2 + y^2 = 1\};$$

而位于该单位圆以外同时又在以原点为中心半径为 2 的圆内的所有点构成的集合是

$$\{(x, y) \in \mathbf{R}_2 \mid x^2 + y^2 > 1 \text{ 且 } x^2 + y^2 < 4\};$$

上述两圆给定后，在小圆内的所有点和在大圆外的所有点一起形成的集合是

$$\{(x, y) \in \mathbf{R}_2 \mid x^2 + y^2 < 1 \text{ 或者 } x^2 + y^2 > 4\}.$$

在人类文明史上，数字 0 的使用是件很了不起的大事，对数学发展有重要作用. 同样，为了方便起见，我们把不含任何元素的集合称为**空集**，它在集合论中也是有重要作用的，记为$\varnothing$. 例如

$$\{x \in \mathbf{R} \mid 2x^2 + 1 = 0\} = \varnothing, \quad \{x \in \mathbf{I} \mid 3x = 5\} = \varnothing.$$

又如，前面提到的青年小组中 20 岁以下青年的集合是空集.

定义 2 设 A, B 都是集合. 说**集合** A 是集合 B 的**子集合**，当而且仅当 A 的每个元素都是 B 的元素. 换句话说，A 是 B 的**子集合**当而且仅当 $x \in A$ 蕴涵着 $x \in B$. 当 A 是 B 的子集合时，记做 $A \subseteq B$，也说是 A 属于 B 或 B 包含 A. 符号 $A \nsubseteq B$ 表示 A 不是 B 的子集.

如果 $A \subseteq B$，但 $A \neq B$，即有 B 的元素不属于 A，则说 A 是 B 的**真子集**，记为 $A \subset B$.

因为空集$\varnothing$不含任何元素，说"$\varnothing$的每个元素 a 都具有某某性质"这句话，从形式逻辑上看，在数学中不会引起矛盾. 于是，我们可以说"$\varnothing$的任意元素都能被 2 整除"，也可以说"$\varnothing$的每个元素都不能被 2 整除"或"$\varnothing$中的每个元素都是要考抽象代数学的青年人"等等. 于是，我们可以约定，对任意集合 A，都有$\varnothing \subseteq A$.

任意集合 A，若 $A \neq \varnothing$，则说 A 是非空集合或 A 非空. 由于

$\varnothing\subseteq A$ 永远成立，当 A 非空时，就有$\varnothing\subset A$.

例题 1 给出集合$\{1,2,3\}$所有子集所形成的集合.

首先要提醒读者，$\varnothing$是这个集合的一个子集，它不含任何元素并不意味着可写可不写.

其次，要知道 A 也是自己的一个子集.

还有，子集$\{1,2\}$和子集$\{2,1\}$是一回事，不要重复开列.

最后，要注意此题答案是唯一确定的，但开列元素的顺序可以不同，下面给出一种写法：

$$\{\varnothing,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}.$$

这里容易犯的错误是把某个数字看成是子集. 我们说，2 是$\{1,2,3\}$的一个元素，而 2 这一个数字所构成的集合$\{2\}$是$\{1,2,3\}$的一个子集.

定义 3 集合 A 的所有子集所形成的集合称为 A 的**幂集**.

定义 4 由任意集合 A,B 决定一个集合

$$\{x\mid x\in A \text{ 或者 } x\in B\},$$

称为 A 和 B 的**并集**，记为 $A\cup B$.

这个定义中"或者"二字是关键词，它是说只要 x 属于 A,B 之一，它就算 $A\cup B$ 的元素，即 $x\in A$ 蕴涵 $x\in A\cup B$，而 $x\in B$ 亦蕴涵 $x\in A\cup B$，x 同时属于 A 和 B 时，也蕴含 $x\in A\cup B$.

例如，

$$\{1,2,3\}\cup\{2,3,4,5\}=\{1,2,3,4,5\},$$

$$\{x\in\mathbf{I}\mid x \text{ 整除 } 8\}\cup\{x\in\mathbf{I}\mid x \text{ 整除 } 12\}$$
$$=\{-12,-8,-6,-4,-2,-1,1,2,3,-3,4,6,8,12\},$$

$$\{(x,y)\in\mathbf{R}_2\mid x^2+y^2<1\}\cup\{(x,y)\in\mathbf{R}_2\mid x^2+y^2>4\}$$
$$=\{(x,y)\in\mathbf{R}_2\mid x^2+y^2<1 \text{ 或者 } x^2+y^2>4\}.$$

定义 5 由任意集合 A,B 可决定一集合

$$\{x\mid x\in A \text{ 同时 } x\in B\},$$

称为 A 和 B 的**交集**，记为 $A\cap B$.

这个定义中的关键词是“同时”二字，它表示 x 既属于 A 又属于 B，两件事同时成立，人们也用“并且”，“而且”等表示这种情形．

例如，

$$\{1,2,3\}\cap\{2,3,4,5\}=\{2,3\}.$$

$$\{x\in\mathbf{I}\mid x\text{ 整除 }8\}\cap\{x\in\mathbf{I}\mid x\text{ 整除 }12\}$$
$$=\{-4,-2,-1,1,2,4\}.$$

$$\{(x,y)\in\mathbf{R}_2\mid x^2+y^2\geqslant 1\}\cap\{(x,y)\in\mathbf{R}_2\mid x^2+y^2\leqslant 4\}$$
$$=\{(x,y)\in\mathbf{R}_2\mid 1\leqslant x^2+y^2\leqslant 4\}.$$

例题 2 如果 A,B 和 C 都是某集合的子集合．证明：

$$(A\cap B)\cup C=(A\cup C)\cap(B\cup C).$$

分析 我们要证明上式左端集合的每个元素都是右端那个集合的元素，同时右端集合的每一个元素都是左端那个集合的元素．

还有，当已知 x 有某些性质，要证 $x\in X\cup Y$ 时，如果 $x\in Y$，当然 $x\in X\cup Y$；如果 $x\notin Y$，我们就要证明必有 $x\in X$．因为“如果 $x\in Y$，当然 $x\in X\cup Y$”一句话恒对，从而不必每次都提起叙述一遍，而直接从“如果 $x\notin Y$，……”入手验证．

证明 对每个 $x\in(A\cap B)\cup C$，由并集的定义知 $x\in A\cap B$ 或者 $x\in C$．

当 $x\in C$ 时，x 当然属于 $A\cup C$，同时，也当然属于 $B\cup C$，即

$$x\in A\cup C\text{ 且 }x\in B\cup C.$$

按交集的定义，$x\in(A\cup C)\cap(B\cup C)$．

当 $x\in A\cap B$ 时，即 $x\in A$ 并且 $x\in B$．所以，$x\in A\cup C$ 并且 $x\in B\cup C$．由交集定义，知 $x\in(A\cup C)\cap(B\cup C)$．

总之，$x\in(A\cap B)\cup C$ 则必有 $x\in(A\cup C)\cap(B\cup C)$．

反之，对任意 $x\in(A\cup C)\cap(B\cup C)$，如果 $x\notin C$，由于 $x\in A\cup C$ 且 $x\in B\cup C$ 可推出 $x\in A$ 且 $x\in B$，也就是 $x\in A\cap B$．

这就证明了 $x\in(A\cup B)\cap(B\cup C)$，则 $x\in(A\cap B)\cup C$． ▎

例题 3 问对于集合的交集和并集是否有如下的规律：对任意集合 A,B 和 C 都有 $(A\cap E)\cup C=A\cap(B\cup C)$．

分析 要否定一个对“任意”A,B 和 C 都成立的命题,我们只要能找到一组确定的 A,B,C 使上式不能成立即可,不必泛泛讲很多不能成立的理由.所选的反例越简单越好.

解 此命题不能对任意集合恒成立.令

$$A=\varnothing,\quad B=\{1\},\quad C=\{1\},$$

则 $A\cap B=\varnothing$, $(A\cap B)\cup C=\{1\}$,而 $B\cup C=\{1\}$, $A\cap(B\cup C)=\varnothing$. ▌

关于集合的并集和交集有很多计算规律,本课程不要求更多地记住它们.本节所列的习题供刚开始接触这些内容的读者加深对概念的理解用.今后直接引用的只有下列几条几乎可说是不证自明的规律,即对任意集合 A,B 和 C,

$$A\cap B=B\cap A,\quad A\cup B=B\cup A,$$

$$(A\cap B)\cap C=A\cap(B\cap C),\quad A\cup(B\cup C)=(A\cup B)\cup C.$$

今后,我们要经常处理若干个集合的交集和并集的问题.这是两个集合情形的推广.

设 J 是一个非空集合(可以有无限多个元素),每个 $j\in J$ 对应集合 S 的一个子集 A_j,则通常说

$$\{A_j\mid A_j\subseteq S,\ j\in J\}$$

是 S 的一个以 J 标号的**子集族**,J 称为**指标集**.

定义 6 设 $\{A_j\mid A_j\subseteq S,\ j\in J\}$ 是 S 的一个子集族,集合

$$\{x\in S\mid \text{对任意 } j\in J \text{ 都有 } x\in A_j\}$$

称为是这个子集族的**交集**,而集合

$$\{x\in S\mid \text{有某个 } j\in J \text{ 使得 } x\in A_j\}$$

称为是该子集族的**并集**,分别记成 $\bigcap\limits_{j\in J}A_j$ 和 $\bigcup\limits_{j\in J}A_j$.

换言之,$\bigcap\limits_{j\in J}A_j$ 是由 S 中属于每个 A_j 的元素形成的集合,$\bigcup\limits_{j\in J}A_j$ 是 S 中至少属于某一个 A_j 的那些元素形成的集合.

例题 4 证明:当 $J=\{1,2,3\}$ 时,$\bigcap\limits_{j\in J}A_j=(A_1\cap A_2)\cap A_3$.

证明 若 $x\in\bigcap\limits_{j\in J}A_j$,则 $x\in A_1$, $x\in A_2$ 而且 $x\in A_3$,从而 $x\in A_1\cap A_2$ 同时 $x\in A_3$,进而 $x\in(A_1\cap A_2)\cap A_3$.

反之,若 $x\in(A_1\cap A_2)\cap A_3$,则 $x\in A_1\cap A_2$ 且 $x\in A_3$,而 $x\in A_1\cap A_2$ 又意味着 $x\in A_1$ 同时 $x\in A_2$,总起来即有 $x\in A_1$, $x\in A_2$,且 $x\in A_3$,即

$$x\in\bigcap_{j=1,2,3}A_j.$$

▌

有时,一个集合的子集族不用标号形式给出,而是描述形式,如

$$\{A\mid A\subseteq S,\ A\neq\varnothing\}$$

乃表示是 S 的所有非空子集形成的族. 同样可把属于该族每个子集的元素形成的集合叫做这族子集的交集,并可相应地定义其并集. 此时,可把描述条件记在符号$\cap$或$\cup$的下边.

例题 5 设 A,B 是集合 S 的子集,它们确定了 S 的一个子集族

$$\mathscr{F}=\{X\mid X\subseteq S,\ A\subseteq X \text{ 且 } B\subseteq X\}.$$

证明:$\bigcap\limits_{A\subseteq X,B\subseteq X}X=A\cup B$.

证明 对任意 $X\in\mathscr{F}$,由 $A\subseteq X$, $B\subseteq X$ 知$A\cup B\subseteq X$,即 $A\cup B$ 的任意元 x 都属于每一个 $X\in\mathscr{F}$,从而 $x\in\bigcap\limits_{X\in\mathscr{F}}X$,即

$$A\cup B\subseteq\bigcap_{A\subseteq X,B\subseteq X}X.$$

另一方面,$A\cup B$ 也满足 $\mathscr{F}$中的描述条件,即 $A\cup B\in\mathscr{F}$. 若 $x\in\bigcap\limits_{X\in\mathscr{F}}X$,则对任意 $X\in\mathscr{F}$都有 $x\in X$,当然应有 $x\in A\cup B$. ▌

例题 6 设 A 是集合 S 的子集. 问,是否必有 $A\subset\bigcap\limits_{X\subset S,A\subset X}X$.

解 此断言不恒对. 例如取 $S=\mathbf{R}$, $A=\{0\}$, $\mathscr{F}=\{X\mid A\subset X\subset S\}$,则

$$\bigcap_{A\subset X\subset S}X=\{0\}=A.$$

这是因为对任意 $a\in\mathbf{R}$, $a\neq0$,都有

$$A\subset\left\{0,\frac{a}{2}\right\}\subset S,$$

即$\{0,a/2\}\in\mathscr{F}$. 但 $a\notin\{0,a/2\}$,从而

$$a \notin \bigcap_{A \subset Y \subset S} X.$$

此事说明族 $\mathscr{F}$ 的交集只含一个元素 0. A 不是它的真子集. ▌

定义 7 设 $A \subseteq B$,那么,集合

$$\{x \mid x \in B \text{ 但 } x \notin A\}$$

称之为 A 在 B 中的**余集**,记为 $B-A$.

例如 $\{1,2,3,4,5\}-\{1,3,5\}=\{2,4\}$.

又如

$$\mathbf{R}_2-\{(x,y)\in \mathbf{R}_2 \mid x^2+y^2\leqslant 1\}=\{(x,y)\in \mathbf{R}_2 \mid x^2+y^2>1\}.$$

例题 7 设 S 是个非空集合,$\mathscr{P}$ 是它的幂集. 证明:对任意 $A,B,C\in\mathscr{P}$ 恒有

$$\{[(A\cup B)-(A\cap B)]\cup C\}-\{[(A\cup B)-(A\cap B)]\cap C\}$$
$$=\{A\cup[(B\cup C)-(B\cap C)]\}-\{A\cap[(B\cup C)-(B\cap C)]\}.$$

分析 这个等式表面上比较复杂,但仔细观察一下,多次出现的乃是两个集合交集在它们的并集中的余集,这种事实用示意图画出来,是相当直观的.

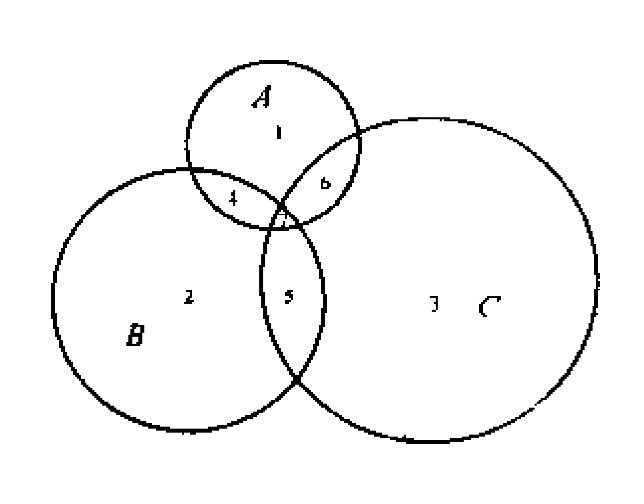


图 1-1

证明 设 A,B,C 如图 1-1. 这个图形由七部分组成:

7 号区域:$A\cap B\cap C$,

4 号区域:$A\cap B-A\cap B\cap C$,

5 号区域:$B\cap C-A\cap B\cap C$,

6 号区域:$A\cap C-A\cap B\cap C$,

1 号区域:A 去掉 4 号、6 号和 7 号区域,

2 号区域:B 去掉 4 号、5 号和 7 号区域,

3 号区域:C 去掉 5 号、6 号和 7 号区域.

所以,我们有(以下数字 1,2,…,7 分别表示第 1、第 2……第 7 号

区域)

$$[(A\cup B)-(A\cap B)]\cup C$$
$$=[(1\cup 2\cup 4\cup 5\cup 6\cup 7)-(4\cup 7)]\cup 3\cup 5\cup 6\cup 7$$
$$=1\cup 2\cup 5\cup 6\cup 3\cup 7, \tag{1}$$

$$[(A\cup B)-(A\cap B)]\cap C$$
$$=(1\cup 2\cup 5\cup 6)\cap(3\cup 5\cup 6\cup 7)$$
$$=5\cup 6, \tag{2}$$

$$A\cup[(B\cup C)-(B\cap C)]$$
$$=(1\cup 4\cup 6\cup 7)\cup[(2\cup 3\cup 4\cup 5\cup 6\cup 7)-(7\cup 5)]$$
$$=(1\cup 4\cup 6\cup 7)\cup(2\cup 3\cup 4\cup 6)$$
$$=1\cup 2\cup 3\cup 4\cup 6\cup 7, \tag{3}$$

$$A\cap[(B\cup C)-(B\cap C)]$$
$$=(1\cup 4\cup 6\cup 7)\cap(2\cup 3\cup 4\cup 6)$$
$$=4\cup 6. \tag{4}$$

于是,可以看出,(2)在(1)中的余集是 $1\cup 2\cup 3\cup 7$;

而(4)在(3)中的余集也是 $1\cup 2\cup 3\cup 7$,命题得证.

这个例子在第二章和第四章还会出现. ▌

习 题 一

1. 用描述方式写出下列集合:

(a) $\{\cdots,-7,-5,-3,-1\}$;

(b) {2 月 1 日,3 月 1 日,4 月 1 日};

(c) $\{1/2,2/3,3/4,4/5,\cdots\}$;

(d) $\{3,1,4,5,9\}$.

2. 将下列集合用列举元素方法写出来:

(a) $\{x\mid x\in\mathbf{I},x\geqslant -6\}$;

(b) $\{x\in\mathbf{I}\mid 1<x<48$ 且 x 为素数$\}$;

(c) $\{(x,y)$为坐标平面上的点$\mid y=2x$ 且 $x^2+y^2=5\}$;

(d) $\{x\in\mathbf{R}\mid x>0$ 且 x 为真分数$\}$;

(e) $\{x$ 代表月份$\mid x$ 不是有 30 天的月份$\}$;

(f)* $\{n\in\mathbf{I}\mid$有正整数 m 使得 $n+1=4m$ 且 $n^2=2m+1\}$.

3. 用 A,B,C 代表三角形三个边上点分别形成的集合，a,b 和 c 代表该三角形的三个顶点. 试给出 $A\cap B, A\cap B\cap C, A\cup B\cup C$.

4. 设 A,B 和 C 都是集合 S 的子集. 证明：若 $A\subseteq B, B\subseteq C$ 且 $C\subseteq A$，则

$$A=B=C.$$

5. 设 $A\subseteq B$, $B\cap C=\varnothing$. 如果 $A\cup C=B\cup C$，则必有 $A=B$.

6. 设 $I_{(n)}=\{-n,-(n-1),\cdots,0,\cdots,n-1,n\}$, $n=1,2,\cdots$. 求 $\bigcup\limits_{n\in I} I_{(n)}, \bigcap\limits_{n\in I} I_{(n)}$.

7. 利用图 1-1，证明：对任意 $A,B,C\in\mathscr{P}$，恒有

$$A\cap[(B\cup C)-(B\cap C)]=(A\cap B)\cup(A\cap C)-(A\cap B\cap C).$$

§2 笛卡尔积和关系

在平面解析几何中，建立笛卡尔坐标系，使平面上每个点都对应一对实数，把几何图形与数量联系起来，即可用代数方法处理几何问题. 这样，几何学可利用代数学的丰富成果，而许多代数问题也因有了几何的讨论才获得明确的解答.

我们把这种“从实数到实数对”的构造方法推广到更一般情形.

定义 1 对任意集合 A 和 B，集合

$$A\times B=\{(a,b)\mid a\in A, b\in B\}$$

称为是 A,B 的**笛卡尔积**，其中

$$(a,b)=(a_1,b_1),\quad a,a_1\in A;\ b,b_1\in B$$

当而且仅当 $a=a_1$, $b=b_1$.

从定义中可以看出，$A\times B$ 和 $B\times A$，在 A,B 不同时，是两个不同的集合. 对于同一个集 A, $A\times A$ 中的元素 (a_1,a_2) 也不能将 a_1 和 a_2 随便颠倒顺序.

例如，若 $A=\{1,2\}$, $B=\{3,4,5\}$，则

$$A\times B=\{(1,3),(1,4),(1,5),(2,3),(2,4),(2,5)\},$$

$$B\times A=\{(3,1),(3,2),(4,1),(4,2),(5,1),(5,2)\}.$$

又如，在一个有 31 排座位，每排 6 个座席的飞机座舱中，其座席号可约定省去“排”、“号”等字样，票上按顺序只打“排序”、“座序”，即用下面集合的元素标明：

$$\{1,2,\cdots,31\}\times\{A,B,C,D,E,F\}$$
$$=\{(1,A),(1,B),\cdots,(31,F)\}.$$

而火车硬席卧铺车中，用以标明铺位的集合可为

$$\{1,2,\cdots,20\}\times\{\text{下},\text{中},\text{上}\}$$
$$=\{(1,\text{上}),(1,\text{中}),\cdots,(20,\text{下})\}.$$

电影院有 40 排座，每排 40 个座位，如果规定(23,4)是排序在第一位置上，座号在第二位置上，则你不能坐到 4 排 23 号位上，这是两个不同的位置.

再如，在实平面上取定坐标系后，若

$$A=\{-1,1\},\quad B=\{1,2\},$$

则 $A\times B$ 乃是图 1－2 上的点集，而图 1－3 上的点集对应 $B\times A$.

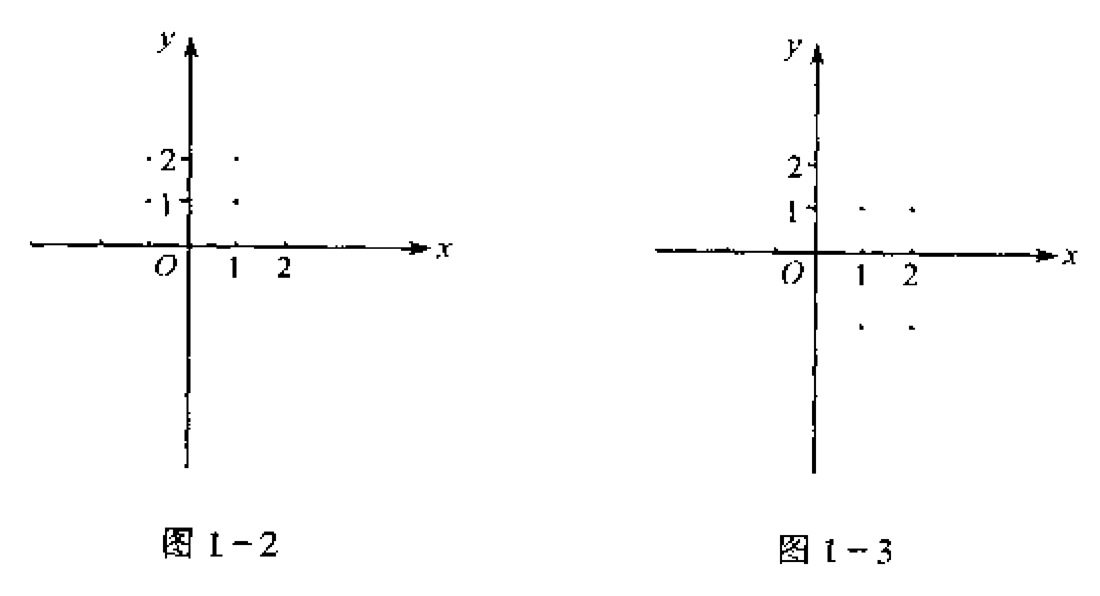


图 1－2　　　　图 1－3

由于空集$\varnothing$不含任何元素，故对任意集合 A 而言，$A\times\varnothing$和$\varnothing\times A$ 也不含任何元素，即

$$A\times\varnothing=\varnothing\times A=\varnothing.$$

因为大家对于实数的笛卡尔积已经在解析几何、线性代数及

普通物理中遇到过，现在接受上述定义应该是不困难的，这里就不再多说了．但是，下面要给出的“关系”这个概念，对相当多的读者来说，是陌生的，同时也是必须深入理解的．

定义 2　设 A 和 B 都是集合．任取笛卡尔积 $A\times B$ 的一个子集 R，我们都说确定了 A 和 B 的一个**关系** R．对任意 $a\in A$，$b\in B$，如果 $(a,b)\in R$，则说 a 与 b 有 R 关系，记为 aRb；如 $(a,b)\notin R$，则说 a 与 b 没有 R 关系．

例 1　设 $A=\{1,2,3,4\}$，$B=\{2,3,4,5,6\}$．若

$$R_1=\{(2,2),(3,3),(4,4)\},$$

即 $2R_12,3R_13,4R_14$，这实际就是大家早已熟悉的整数的相等关系．也就是说 A 中元素 a 和 B 中元素 b 有 R_1 关系当而且仅当 $a=b$．

如果，

$$R_2=\{(1,2),(1,3),(1,4),(1,5),(1,6),(2,3),(2,4),(2,5),(2,6),(3,4),(3,5),(3,6),(4,5),(4,6)\},$$

即 $1R_22,1R_23,\cdots,4R_26$．仔细分析一下，即知 A 中元素 a 与 B 中元素 b 有 R_2 关系当而且仅当，作为整数，a 小于 b，即 $a<b$．

同理，取

$$R_3=\{(3,2),(4,2),(4,3)\},$$

那么 aR_3b 当而且仅当 $a>b$．

而取 $R_4=\{(1,2),(2,4),(3,6)\}$ 时，容易看出，aR_4b 充分必要条件是 $2a=b$．

从此例可以看出，这里给出的“关系”的定义是符合人们习惯的，是有背景的．

例 2　设 A 为 20 岁以上中国公民形成的集合，B 是我国 29 个省市形成的集合，则

$$R=\{(a,x)\in A\times B\mid a\text{ 在 }x\text{ 逗留过 48 小时以上}\}$$

是 A 与 B 的一个关系．

例 3　实平面 $\mathbf{R}\times\mathbf{R}$ 中，图 1－4内两个圆周上的所有点形成的集合记为 S，则对任意实数 x,y，xSy 即 $(x,y)\in S$ 的充分必要条件是 $x^2+y^2=1$ 或者

$$(x-1)^2+y^2=1.$$

注意，这个定义中，$A\times B$ 的子集 R 取定后，$A\times B$ 的每个元素是否属于 R 就是完全确定的，任意 $(a,b)\in R$ 或 $(a,b)\notin R$ 必居其一，也就是说 a 和 b 有 R 关系或没有 R 关系是完全确定的事情.

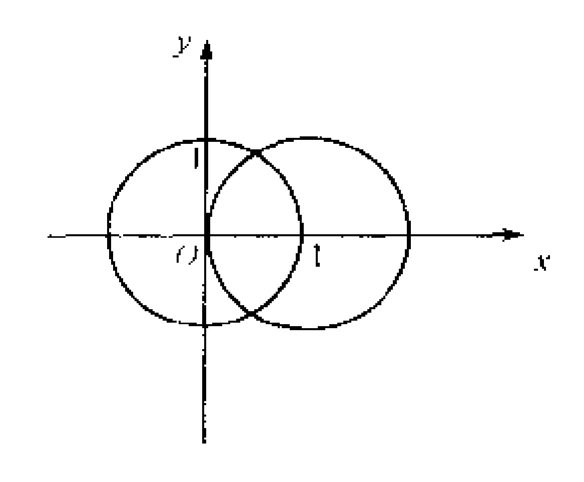


图 1－4

生活中或其他学科中有些不明确的说法，在完成数学上的精确化之前，不能认为是符合我们的"关系"定义的.

例如，设 $A=\{$王甲，李乙，赵丙$\}$，$B=\{$数学分析，线性代数，抽象代数学，统计数学$\}$. 如果用如下的性质确定 $A\times B$ 的子集：

$$a\in A,\ b\in B,\ a \text{ 较好地掌握了 } b \text{ 知识},$$

事情是很难办的，因为"很好"、"较好"、"掌握"等概念不明确，你无法确定每个 (a,b) 是否满足要求，也就是说这不是个确定的子集.

只要明确定义"所谓较好掌握该知识是指经过省级考试，成绩达到……或在本领域实践中取得……等级成果者"，此时

$$R=\{(a,b)\mid(a,b)\in A\times B, a \text{ 较好掌握 } b \text{ 的知识}\}$$

才是 $A\times B$ 的一个子集，从而确立了 A 与 B 之间的一个关系.

在数学的各个分支中最常用到的是例 3 中那种 $A=B$ 的情形，此时 $A\times A$ 的一个子集 R 确定 A 和 A 的一个关系，就可以简单说是确定 A 的一个关系. 具体说来，对任意 $a,b\in A$，说 a 和 b 有 R 关系，当而且仅当 $(a,b)\in R$.

很明显，所说的 a、b 是有顺序的，a 和 b 有关系并不意味着 b 和 a 一定有 R 关系.

设 A 为一集合.笛卡尔积 $A\times A$ 的子集 R 用条件 P 描述,即

$$R=\{(a,b)\in A\times A\mid(a,b)\text{满足 }P\text{ 条件}\}.$$

由于 $A\times A$ 的元素 (a,b) 满足 P,也可以说成是,A 的两个(有顺序的)元素 a,b 满足 P,故下列说法是等价的:

(1) $(a,b)\in R$;

(2) $(a,b)\in A\times A$, (a,b)满足 P;

(3) $a,b\in A$, a 和 b 满足 P.

比如,例 3 中,xSy 必要而只要 (x,y) 满足

$$x^2+y^2=1\text{ 或 }(x-1)^2+y^2=1,$$

必要而只要 x,y 满足

$$x^2+y^2=1\text{ 或 }(x-1)^2+y^2=1.$$

又如,平面 $\mathbf{R}\times\mathbf{R}$ 上阴影部分,即直线

$$y=x$$

的下方点集 S,确定了一个关系 S,则下面两个说法是等价的

(2) $(x,y)\in\mathbf{R}\times\mathbf{R}$, $y<x$;

(3) $x,y\in\mathbf{R}$, $y<x$.

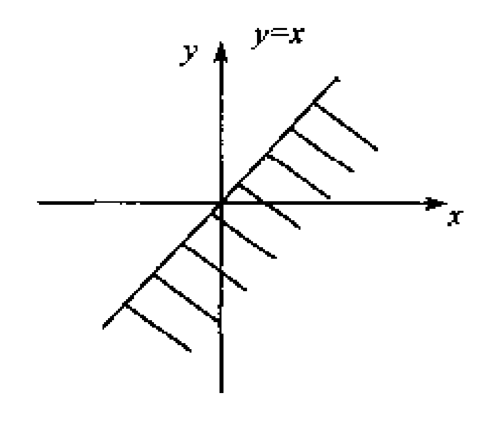


图 1-5

由于(3)中不涉及笛卡尔集概念,有时叙述起来简洁些.所以,某些时候,我们也用这种方式来定义关系.

设有任意 n 个集合 $A_1,A_2,\cdots,A_n$.我们称集合

$$\{(a_1,\cdots,a_n)\mid a_1\in A_1,\cdots,a_n\in A_n\}$$

为集合 $A_1,\cdots,A_n$ 的**笛卡尔积**,并记为

$$A_1\times A_2\times\cdots\times A_n.$$

例如,n 元实数行

$$(r_1,r_2,\cdots,r_n)$$

所构成的集合可记为 $\mathbf{R}\times\cdots\times\mathbf{R}$.

习 题 二

1. 给出下列情形中的笛卡尔积 $A\times B$:

(a) $A=\{1,2\}$, $B=\{1,2,3\}$;

(b) $A=\{1\}$, $B=\{1,2,3,4,5,6\}$;

(c) $A=\{x\in\mathbf{R}\mid x\leqslant 0\}$, $B=\{y\in\mathbf{R}\mid y\geqslant 1\}$;

(d) $A=\{x\in\mathbf{R}\mid x\leqslant 0\}$, $B=\mathbf{I}$;

(e) $A=\{x\in\mathbf{I}\mid 1\leqslant x\leqslant 6\}$, $B=\{y\in\mathbf{I}\mid 0<y<2\}$;

(f) $B=\{x\in\mathbf{I}\mid x\leqslant 0\}$, $A=\mathbf{I}$;

(g) $A=B=\{1,2\}$;

(h) $A=\{1,2\}\times\{1,2\}$, $B=\{1,2\}$;

(i) $A=\{1,2\}$, $B=\{1,2\}\times\{1,2\}$.

2. 设 $A=\{0,2\}$, $B=\{9,10,11,12,13\}$. 对下列给出的 $A\times B$ 的子集 R 确定的关系做些解释:

(a) $R=\{(2,10),(2,12)\}$;

(b) $R=\{(0,9),(0,11),(0,13),(2,9),(2,11),(2,13)\}$;

(c) $R=\{(0,10),(2,12)\}$.

3. 设 $A=\{x\in\mathbf{I}\mid 2\leqslant x\leqslant 12\}$. 对下列 A 上的关系 R 给出 $A\times A$ 的子集:

(a) xRy 当且仅当 x 是 y 的真因子;

(b) xRy 当且仅当 $x+y=21$;

(c) xRy 当且仅当 $y=2x+1$.

4. 设 $A=\{-1,0,1,2,3,4\}$, $B=\{1,2,3,4,5\}$. 试用列举元素方法写出关系: $\{(a,b)\in A\times B\mid |b^2-a|=2\}$.

§3 等价关系、分类和商集

在各种关系中,下面要讨论的所谓等价关系是最重要而又有用的一种,它与集合的元素分类问题密切相关.

定义 1 设 R 是集合 A 上的一个关系,也就是 $R\subseteq A\times A$. 若它满足下列三条性质:

(1) 反身性,即对任意 $a\in A$ 都有 aRa;

(2) 对称性,即对任意 $a,b\in A$, aRb 蕴涵 bRa;

(3) 传递性,即对任意 $a,b,c\in A$,如果有 aRb, bRc 则必有 aRc,则说 R 是 A 上一个**等价关系**.

例 1 在整数集 $\mathbf{I}$ 上,令

$$R=\{(a,b)\in\mathbf{I}\times\mathbf{I}\mid a-b \text{ 为偶数}\}.$$

则 R 确定 $\mathbf{I}$ 上一个等价关系.

证明 对任意整数 a, $a-a=0$, 0 为偶数,故 aRa;

对任意整数 a,b,如果 aRb,即 $a-b$ 为偶数,则 $b-a$ 也是偶数,从而 bRa;

对任意 $a,b,c\in\mathbf{I}$,如果 aRb, bRc,即 $a-b$ 为偶数, $b-c$ 为偶数,从而

$$a-c=(a-b)+(b-c)$$

亦为偶数,也就是 aRc.

这个例子可以推广到更一般情形,对一个固定的自然数 n,令

$$R_n=\{(a,b)\in\mathbf{I}\times\mathbf{I}\mid a-b \text{ 为 } n \text{ 的倍数}\},$$

则 R_n 确定 $\mathbf{I}$ 上一个等价关系.

例 2 设 A 是所有 m 阶实方阵形成的集合,则下面 $R_1,R_2,R_3\subseteq A\times A$ 分别确定 A 上等价关系:

$$R_1=\{(a,b)\in A\times A\mid \text{有非奇异方阵 } P,Q \text{ 使 } PaQ=b\},$$

$$R_2=\{(a,b)\in A\times A\mid \text{有非奇异方阵 } P \text{ 使得 } PaP^{-1}=b\},$$

$$R_3=\{(a,b)\in A\times A\mid a \text{ 的对角线元素之和等于 } b \text{ 对角线元素之和}\}.$$

例 3 设 A 为某寝室学生的集合,令

$$R_1=\{(a,b)\in A\times A\mid a,b \text{ 听过同一老师的课}\},$$

R_1 确定 A 上一个关系,但不是等价关系.可能甲和乙在二年级听过同一老师的课,而乙和丙也同时听过另一老师的课,但甲和丙却从来没有机会听同一老师的课.即不满足传递性.

这个例子中,如果 A 是某居民委员会居民构成的集合,那么 R_1 可能不满足反身性,也许有人没听过任何老师讲课.

如果在该例中,A 仍为某寝室学生的集合而

$$R_2=\{(a,b)\in A\times A \mid a,b \text{ 于 1989 年度选学完全一致的学习科目}\},$$

则 R_2 是 A 上等价关系.

上节说过,我们既可以用笛卡尔积 $A\times A$ 中元素(a,b)来叙述一个给定的关系,也可用集合 A 中元素 a 和 b 来叙述该关系. 习惯上,人们引入特殊符号"$\sim$"表示一个等价关系,故有

定义 1* 设$\sim$是集合 A 上一个关系. 若它满足下列三条性质:

(1)* 反身性,即对任意 $a\in A$,都有 $a\sim a$;

(2)* 对称性,即对任意 $a,b\in A$, $a\sim b$ 蕴涵 $b\sim a$;

(3)* 传递性,即对任意 $a,b,c\in A$,如果 $a\sim b,b\sim c$ 则必有

$$a\sim c,$$

则说$\sim$是 A 上的一个等价关系.

例 4 几何空间中,规定直线 $L_1\sim L_2$ 当而且仅当 L_1 平行或等于 L_2,则$\sim$为等价关系.

例 5 所有在区间$[-1,1]$上连续的函数构成集合为 A,规定 $f(x)\sim g(x)$当而且仅当

$$\int_{-1}^{1}f(x)\mathrm{d}x=\int_{-1}^{1}g(x)\mathrm{d}x,$$

则$\sim$为等价关系.

等价关系之所以到处可见,是因为它与下面要讨论的分类问题密切相关,而分类是所有科学研究工作中都采用的方法. 只有把研究对象按特定要求分门别类,才能区别各种事物间的本质差异.

定义 2 设$\sim$是集合 A 上的一个等价关系,对每个 $x\in A$,称 A 的子集

$$S_x = \{y \mid y \sim x\}$$

为元素 x 的**等价类**.

命题 1 符号如定义 2 所设,则对于任意 $x \in A$, S_x 非空;对任意 $x, y \in A$,若 $S_x \neq S_y$ 则必有 $S_x \cap S_y = \varnothing$; A 恰为其所有不同的等价类的并集.

证明 对任意 $x \in A$,由于 $\sim$ 是等价关系,故 $x \sim x$,即

$$x \in S_x, \quad S_x \neq \varnothing.$$

如果 $S_x \cap S_y \neq \varnothing$,设 $z \in S_x \cap S_y$. 由定义知 $z \sim x$ 且 $z \sim y$. 由于 $\sim$ 是等价关系,由 $z \sim x$ 推出 $x \sim z$. 再由 $x \sim z$, $z \sim y$ 推出 $x \sim y$. 于是,对任意 $w \in S_x$,因为 $w \sim x$,又推知 $w \sim y$, $w \in S_y$. 从而 $S_x \subseteq S_y$. 完全对称地,又必有 $S_y \subseteq S_x$. 进而得 $S_x = S_y$. 这说明,两个等价类或相同或不相交.

由于每个 $x \in A$, $x \in S_x$,所以

$$A = \bigcup_{x \in A} S_x.$$

把其中重复的相同的等价类删去,则 A 为其不同的等价类的并集. ▌

一个集合 B,如果有以 Δ 为标集的子集族 $\{T_i \mid i \in \Delta\}$,对任意 $i \in \Delta$,有 $T_i \neq \varnothing$,且

(1) $T_i \cap T_j = \varnothing$,只要 $i \neq j$,

(2) $B = \bigcup_{i \in \Delta} T_i$,

则说这是 B 的一个**分类**,也叫**分划**.

它的含义是,B 中的每个元素必然分到一个子集 T_i 中去,而且只能在一个 T_i 中.

例 6 北京市正式居民按户籍所在区县论,即得一分类. 每居民必属一个区县,且无任何居民同时属不同两区县.

例 7 n 阶实方阵按秩数论,得 n 阶方阵一分类.

例 8 一个单位中的成员,按年龄、性别、血型,都得一分类. 按所属党派论,未必能得我们讨论意义下的分类,因为有人可能同

时属于两个不同党派.

命题 1 证明了:给定集合 A 上一个等价关系,就给了 A 一个分类.

反过来,还有

命题 2 若有集合 A 的一个分类,即有 A 的子集族 $S_i, i\in\Delta$ 满足

(1) $S_i\cap S_j=\varnothing,\ i\neq j,$

(2) $A=\bigcup\limits_{i\in\Delta}S_i,$

规定,对任意 $a,b\in A$, $a\sim b$ 当而且仅当 a 与 b 属于同一 S_i. 则 $\sim$ 为 A 上等价关系,且诸 S_i, $i\in\Delta$ 恰为 $\sim$ 对应的不同的等价类.

证明 因为 $A=\bigcup\limits_{i\in\Delta}S_i$,对任意 $a\in A$,必有 $i\in\Delta$, $a\in S_i$,从而 $a\sim a$. 即 $\sim$ 有反身性.

对称性是显然的.

设 $a\sim b$ 且 $b\sim c$,即有 $i,j\in\Delta$,

$$a,b\in S_i,\quad b,c\in S_j.$$

由 $b\in S_i\cap S_j$ 知 $i=j$,从而 $a,c\in S_j$, $a\sim c$. 即 $\sim$ 有传递性.

再来证明每个 S_i 恰为 $\sim$ 之下的一个等价类. 由于 S_i 非空,设 $x\in S_i$,我们断言

$$S_i=S_x.$$

首先,对任意 $y\in S_x$, $y\sim x$,由于已假定 $x\in S_i$,据 $\sim$ 的定义,知 $y\in S_i$. 这说明 $S_x\subseteq S_i$. 另一方面,对任意 $z\in S_i$,由于已经有 $x\in S_i$,故 $z\sim x$,从而 $z\in S_x$,这说明 $S_i\subseteq S_x$. 所以,$S_i=S_x$. ▌

例 9 在整数集 $\mathbf{I}$ 上,规定 $a\sim b$,当而且仅当 $a-b$ 为偶数. 这是个等价关系,且

$$S_{-1}=S_1=S_3=\{x\in\mathbf{I}\mid x\text{ 为奇数}\},$$

$$S_{-2}=S_0=S_2=\{x\in\mathbf{I}\mid x\text{ 为偶数}\}.$$

所以,$\sim$ 决定 $\mathbf{I}$ 的一个分类,即 $A=\mathbf{I}$,

$$A=S_1\cup S_2,\quad S_1\cap S_2=\varnothing.$$

当然,你愿意写 $A=S_{18}\cup S_{-9}$ 也可以,因为 S_{18} 与 S_2 是 A 的同一个子集,S_{-9} 与 S_1 是同一个子集,前者均为偶数集,后者都是奇数集.这个分类就是把整数集分成奇数集和偶数集这样不相交的两个子集.

例 10 在所有实系数多项式作成的集合 P 上,规定 $f(x)\sim g(x)$ 当而且仅当 $f'(x)=g'(x)$.这也是一个等价关系.由于 $f'(x)=g'(x)$ 必要而只要 $f(x)$ 与 $g(x)$ 相差一常数,故

$$S_{f(x)}=\{g(x)\in P\mid g(x)=f(x)+C,\ C\in\mathbf{R}\}.$$

定义 3 设~是集合 A 上的一个等价关系,说 A 的子集 T 是关系~下的一个**等价类表示的完全集**(简称**完全集**),如果 T 中不同的元素的等价类也不同,且 $A=\bigcup\limits_{t\in T}S_t$.

例 7 中,n 个矩阵

$$\begin{pmatrix}1&&&&\\&0&&&\\&&0&&\\&&&\ddots&\\&&&&0\end{pmatrix},\begin{pmatrix}1&&&&\\&1&&&\\&&0&&\\&&&\ddots&\\&&&&0\end{pmatrix},\cdots,\begin{pmatrix}1&&&&\\&1&&&\\&&1&&\\&&&\ddots&\\&&&&1\end{pmatrix}$$

是个完全集.例 9 中 $\{1,2\}$ 是个完全集,同时 $\{-9,18\}$ 也是完全集.例 10 中

$$T=\{f(x)\in P\mid f(x)=a_0x^n+\cdots+a_{n-1}x+1\}$$

构成一个完全集.这是因为任意一个多项式

$$g(x)=b_0x^m+b_1x^{m-1}+\cdots+b_{m-1}x+b_m$$

必等价于 $b_0x^m+\cdots+b_{m-1}x+1\in T$,即必有 $t\in T$ 使 $g(x)\in S_t$.

另一方面,若 $h(x),k(x)\in T$, $h'(x)=k'(x)$,则必有实数 b 使 $h(x)=k(x)+b$.但 $h(x)$ 和 $k(x)$ 的常数项均为 1,故必有 $b=0$, $h(x)=k(x)$.也就是说,当 $k\neq h$ 时,$S_k\cap S_h=\varnothing$.

定义 4 设~是集合 A 上的等价关系,T 是关系~之下的一

个完全集，则集合

$$\bar{A}=\{S_t \mid t\in T\}$$

称为对等价关系～的**商集**.

要注意的是，$\bar{A}$ 是以等价类为元素，T 是以等价类中代表元为元素，绝不可混为一谈. $\bar{A}$ 是由～唯一确定的，而完全集可能有很多.

比如，例 9，$A=\mathbf{I}$，对于～，商集

$$\bar{A}=\{S_1,S_2\}=\{S_{18},S_{-9}\}.$$

$\bar{A}$ 包含两个元素，每个元素有很多不同的记法，但作为集合，$S_1=S_{-9}=\cdots$都是奇数集 G，而 $S_2=S_0=S_{18}=\cdots$都是偶数集 E. 即

$$\bar{A}=\{G,E\}.$$

如果用列举元素法来写，则

$$\bar{A}=\{\{\cdots,-1,+1,3,\cdots\},\{\cdots,-2,0,2,\cdots\}\}.$$

而 A 对于～的等价类表示完全集却有很多，不是表示法或记号不同，而是不同的集合. 如，$\{0,1\}$是完全集，$\{-9,18\}$是完全集，$\{-39,108\}$也是完全集.

完全集中的元素是整数，而商集中的两个元素分别是两个数集.

本节概念较多，它们是今后讨论的基础，读者必须准确地掌握其表达方式和内在含义.

我们再给一个例题，把所提出的概念串在一起，以利对照比较.

例 11 设数集 A 是

$$\{-2,-1,0,1,2,5,7\}.$$

给定 $A\times A$ 的子集 R 为

$$\{(-2,-2),(-2,1),(-2,7),(1,-2),(1,1),(1,7),\\(7,1),(7,7),(7,-2),(2,2),(2,5),(5,2),(5,5),\\(-1,-1),(-1,2),(-1,5),(5,-1),(2,-1),(0,0)\},$$

则得 A 上一个关系 R.

由于

$(7,7),(-2,-2),(-1,-1),(0,0),(1,1)(2,2),(5,5)$
均在 R 中,关系 R 有反身性.

容易看出 R 中元素是对称地出现的,R 含 $\{5,2\}$ 同时含 $(2,5)$, R 含 $(1,7)$ 同时含 $(7,1)$…….关系 R 有对称性.

R 也具有传递性.

所以,R 是个等价关系.

这个关系还可以用描述方法给出,

$$R=\{(a,b)\in A\times A \mid a-b \text{ 是 } 3 \text{ 的倍数}\}.$$

也可以 A 中元素来描述,即,对任意 $a,b\in A$, aRb 当而且仅当 $a-b$ 是 3 的倍数.

用最后这种说法时,验证反身性、对称性和传递性会更方便.

现在用 $\sim$ 代替 R.计算等价类,得

$$S_{-2}=\{-2,1,7\},\quad S_1=\{-2,1,7\},$$
$$S_7=\{-2,1,7\},\quad S_2=\{2,-1,5\},$$
$$S_5=\{2,-1,5\},\quad S_{-1}=\{2,-1,5\},$$
$$S_0=\{0,0\}.$$

即 $S_2=S_5=S_{-1}$, $S_{-2}=S_1=S_7$.

于是,等价关系 $\sim$ 把集合 A 分成了 3 类,

$$A=S_{-2}\cup S_2\cup S_0=\{-2,1,7\}\cup\{-1,2,5\}\cup\{0\}.$$

假若,在 A 给定之后,即指定上述分类方式,我们规定属于 $\{-2,1,7\}$ 者有关系,属于 $\{-1,2,5\}$ 者有关系,0 与 0 有关系,得到的这个关系就是 R.

等价关系 R 决定了 A 的一个分类,也决定了 A 的商集

$$\overline{A}=\{\{-2,1,7\},\{-1,2,5\},\{0\}\}.$$

它有 3 个元素,每个元素是集合 A 的一个子集.这里排列在第 3 位的元素 $\{0\}$,同样是一个子集,只不过是该子集只含一个数字 0 而已,不可以把 $\overline{A}$ 写成

$$\{\{-2,1,7\},\{-1,2,5\},0\},$$

或者

$$\{-2,1,7;-1,2,5;0\},$$

等等.

由于 $S_{-2}=S_1=S_7$, $S_{-1}=S_2=S_5$,所以

$$A=S_{-2}\cup S_{-1}\cup S_0=S_1\cup S_5\cup S_0=\cdots$$

有很多种不同的写法,S_{-2},S_{-1} 和 S_0 是两两不同的等价类,S_1,S_5 和 S_0 也是两两不同的等价类.所以,$\{-2,-1,0\}$是个完全集,$\{1,5,0\}$是个完全集,$\{7,2,0\}$也是个完全集.

例 12 设 n 为一正整数,在整数集 **I** 中定义关系～, $a\sim b$ 当而且仅当 $a-b$ 是 n 的整数倍,并将这个关系称为**整数模 n 关系**.有

$$S_0=\{\cdots,-n,0,n,\cdots\},$$
$$S_1=\{\cdots,-n+1,1,n+1,\cdots\},$$
$$\cdots,$$
$$S_{n-1}=\{\cdots,-1,n-1,2n-1,\cdots\}$$

构成 **I** 的一个分类. $\{0,1,\cdots,n-1\}$是 **I** 对于关系～的一个完全集.

当然,$\{-1,0,2,3,\cdots,n-2,n+1\}$也是个完全集.但前者说起来更方便些.

我们令

$$[0]=S_0,\ [1]=S_1,\ \cdots,\ [n-1]=S_{n-1},$$

则 **I** 对于等价关系～的商集是

$$\mathbf{I}_{\sim n}=\{[0],[1],\cdots,[n-1]\}.$$

特别地,

$$\mathbf{I}_{\sim 2}=\{\text{偶数集},\text{奇数集}\}.$$

习　题　三

1. 列举子集 R 的元素分别给出各集合上的相应 R 关系:

(a) 集合$\{1,3,5,7,9\}$上数的"小于"关系；

(b) 集合$\{2,3,4,5,6\}$上数的"互素"关系；

(c) 集合 $B=\{x,y\}$，A 是 B 的所有子集所构成的集合，A 上"包含$\subseteq$"关系.

2. 在下述"证明"中找出漏洞：

现断言，若 A 上关系 R 有对称性和传递性，则必有反身性.

对任意 $a\in A$，由对称性知，若 aRb，则必 bRa. 再由传递性知，aRb 且 bRa 蕴涵着 aRa. 而 a 是任意的，这说明 R 有反身性.

3. 给出一个关系，它有对称性、传递性，但无反身性.

给出一个关系，它有反身性、对称性，但无传递性.

给出一个关系，它有反身性和传递性，但无对称性.

4. 设 $R,S\subseteq A\times A$ 且 R 和 S 都是 A 上的等价关系. 证明：$R\cap S$ 也确定 A 上等价关系.

5* 设 $R_n\subseteq A\times A$，$n=1,2,\cdots$都确定 A 上等价关系，且 $R_n\subseteq R_{n+1}$. 证明：$R=\bigcup_{n\in\mathbf{N}}R_n$ 亦为 A 上的一个等价关系.

6. 设集合 A 只含两个元素. 问，

(a) A 上有多少个不同的关系？

(b) A 上有多少个等价关系？

(c) A 上有多少个关系有对称性？

(d) A 上有多少个关系有传递性？

(e) A 上有多少个关系有反身性？

(f) 集合 A 有几种分类？

§4 映　　射

设 A,B 是集合.

在 A 和 B 的各种各样的关系中，有一类特殊的关系，也就是 $A\times B$ 的一类特殊子集 R，对任意 $a\in A$，都有而且只有一个 $b\in B$，使

$$(a,b)\in R.$$

我们暂称这类关系为**映射关系**，在以后的各章节中并不使用这个

称呼.

例如,设 $A=\{9,4,1\}$, $B=\{3,5,8\}$,

$$R=\{(9,3),(4,5),(1,5)\}.$$

A 的所有元素都在 R 中元的第一个位置上出现过(即由 B 中元,与它组成一个 R 中元),而且只出现一次(对每个 $a\in A$,只有一个 b 使 $(a,b)\in R$),这是个映射关系.

这里对于 B 要求较宽松,它的元素可能出现在 R 某个元素中,也可能不出现,如数 8 就没出现.有的元素 $b\in B$ 也可能多次出现在 R 的元素中,如这里的数 5 就出现了两次.

又如,A 和 B 都是整数集 $\mathbf{I}$,

$$R=\{(a,b)\in A\times B\mid a^2=b\}$$

也是一个映射关系.A 中任意元素,必出现在

$$(1,1),(-1,1),(0,0),(2,4),\cdots$$

的第一个位置上,而且只出现一次.

再如,A 是某单位全体在职职工构成的集合,$B=\{x\in\mathbf{I}\mid 14\leqslant x\leqslant 80\}$,则

$$R=\{(a,b)\in A\times B\mid a\text{ 的年龄为 }b\}$$

也是一个映射关系.因为每个职工都有年龄,而且是 B 中唯一确定的数.

但是,当 A 和 B 都是整数集 $\mathbf{I}$ 时,

$$R=\{(a,b)\in A\times B\mid a=b^2\}$$

不是映射关系.因为 $3\in\mathbf{I}$,但对任何 $b\in\mathbf{I}$ 都有 $b^2\neq 3$,即 R 中任何元的第一个数字均不为 3, $(3,b)\notin R$.

此例中,B 仍为整数集,而 A 为平方数集,即

$$A=\{0,1,4,9,\cdots\},$$

那么,

$$R=\{(a,b)\in A\times B\mid a=b^2\}$$

是不是映射关系呢?否.因为 $A\times B$ 的元素

$$(4,2),\quad (4,-2)$$

均在 R 中,4 出现了两次.

进一步,设 A 为平方数集,B 为非负整数集,则

$$R=\{(a,b)\in A\times B \mid a=b^2\}$$

为映射关系.

同样,设 A 为平方数集,B 为非负实数集,那么

$$R=\{(a,b)\in A\times B \mid a=b^2\}$$

亦为映射关系,尽管有些 $b\in B$ 不会出现在 R 的任何元素中(如 $\sqrt{2}$).

形象地说,A 为横轴,B 为纵轴,$A\times B$ 为平面. $A\times B$ 的子集 R (由 $A\times B$ 平面上的点组成)确定 A 和 B 的一个映射关系,当而且仅当,对任意 $a\in A$,直线 $x=a$ 上都有且只有一点 b,使得 $(a,b)\in R$.

容易看出,映射关系包含了人们已经熟悉的变量之间的函数关系.

由于 A 和 B 的关系也可以避开 $A\times B$ 的子集 R 这样的提法,而说 A 和 B 的元素的对应,通常人们习惯于用如下的定义来推广函数概念.

定义 1 设 A,B 是集合. 如果有一对应规则 f,对于集合 A 中任何一个元素 a,在集合 B 中都有唯一的元素 b 和它对应,这个对应叫做从集合 A 到集合 B 的**映射**,记作

$$f:A\to B.$$

f 使集合 A 中元 a 对应 b,记为 $f(a)=b$,也说是 f 把 a 变成 b.

定理 1 如果 R 是集合 A 和集合 B 的一个映射关系,对任意 $a\in A$,有唯一确定的 $b\in B$ 使 $(a,b)\in R$. 我们规定 a 对应这个 b,并把此规则称为 f,则 f 是 A 到 B 的映射.

反之,若 f 是集合 A 到集合 B 的一个映射,令

$$R=\{(a,b)\in A\times B \mid b=f(a)\}$$

就得到 A 和 B 的一个映射关系.

证明 如果 R 是 A 和 B 的一个映射关系. 对任意 $a\in A$,都

有而且只有一个 $b\in B$，使得

$$(a,b)\in R,$$

这个 b 是由 a 唯一确定的. 令 a 对应 b，并记 $b=f(a)$，则 f 是 A 到 B 的映射.

反之，如果 f 是 A 到 B 的映射，那么子集

$$R=\{(a,b)\in A\times B \mid b=f(a)\}$$

中，对任意 $a\in A$，必有唯一确定的 b，使

$$b=f(a).$$

从而 $(a,b)\in R$，即对每个 $a\in A$ 都有唯一确定的 b 使 $(a,b)\in R$. 从而 R 为映射关系. ▌

可以举一简单例子来说明上述两种思想方法之间的联系.

设 $A=\{a,b,c\}$，$B=\{1,2,3,4\}$. 那么，对应规则

$$f(a)=1,\ f(b)=3,\ f(c)=1$$

是 A 到 B 的映射. 如图 1－6，其左侧是 A，其右侧是 B. A 中每个元都有而且只有一个射线发出.

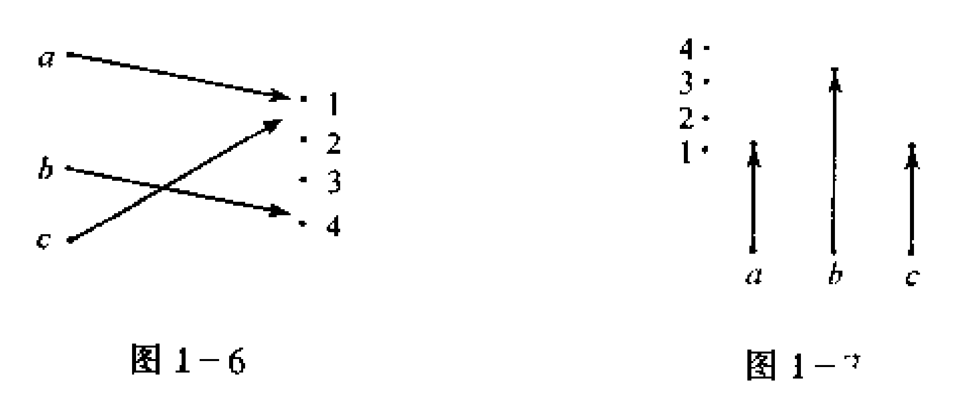


图 1－6　　　　图 1－7

这个事实在 $A\times B$ 中讨论，该映射 f 在 $A\times B$ 中确定子集 R，A 中的每个元素都出现在 R 元素的第一个位置上，而且只出现一次. 如图 1－7 所示，R 中三个元素是由 A 中元和 B 中元给出的，A 中每个元都有而且只有一条射线发出，其终点是 $(a,f(a))$，$(b,f(b))$ 和 $(c,f(c))$，也就是 $(a,1)$，$(b,3)$，$(c,1)$.

由于映射是个对应规则，同一规则可能用不同的方式或顺序叙述出来. 只要"对应"的效果相同，我们就认为是相同的映射.

精确地说，设 $f:A\to B$，$g:C\to D$，认为 f 和 g 相等（记为 $f=g$）当而且仅当 $A=C$ 且 $B=D$ 同时对任意 $a\in A=C$，都有

$$f(a)=g(a).$$

比如，$A=\{1,2\}$，$B=\{4,5,6\}$，则

$$f(1)=4,\quad f(2)=5,$$

与

$$g(2)=5,\quad g(1)=4,$$

是相同的，即 $f=g$. 同样，令

$$h(a)=a+3,\quad a\in A$$

和

$$k(a)=1+4a-a^2,\quad a\in A.$$

则 f,g,h,k 都相等.

但是，若 $D=\{4,5,6,7\}$，映射 $j:A\to D$ 规定为 $j(1)=4$，$j(2)=5$. 我们不能说 $f=j$.

例 1 设 A 是个集合. 规定，任意 $a\in A$ 对应 a 自己. 这是 A 到 A 的映射，称为 A 上的**恒等映射**，记为 i_A，即对任意 $a\in A$ 都有 $i_A(a)=a$，有时把 i_A 中的 A 省略，简记为 i.

例 2 设 A 是集合 B 的一个子集. 规定，任意 $a\in A$ 对应 B 中元素 a. 这是 A 到 B 的映射，把 A 中元变成其自己，称为 A 到 B 的**嵌入映射**，记为 l_A. 即，对任意 $a\in A$，都有 $l_A(a)=a$.

例 3 设 A,B 是集合. 规定，任意元素 $(a,b)\in A\times B$ 对应 a. 这是笛卡尔积 $A\times B$ 到 A 的映射，记为 p_A，即 $p_A((a,b))=a$，对任意 $(a,b)\in A\times B$. 该映射称为 $A\times B$ 到 A 的**投影**. 同样，规定

$$p_B((a,b))=b,\quad (a,b)\in A\times B,$$

得到 $A\times B$ 到 B 的投影.

例 4 设 $\sim$ 是集合 A 上的一个等价关系，$\bar{A}$ 是 A 对 $\sim$ 的商集. 规定，任意 $a\in A$，对于其所在的等价类

$$S_a=\{x\in A \mid x\sim a\},$$

则得到 A 到商集 $\bar{A}$ 的一个映射 γ,

$$\gamma(a)=S_a,\quad 对任意\ a\in A.$$

这个映射称之为由等价关系～决定的自然映射.

特别地,对于自然数集 $\mathbf{I}$ 上的等价关系～, $a\sim b$ 当且仅当 n 整除 $a-b$,我们用 $\mathbf{I}_{\sim n}$ 代表关系～决定的商集.此时由～决定的自然映射 γ 对任意 $m\in\mathbf{I}$ 有

$$\gamma(m)=S_m=\{\cdots,m-n,m,m+n,m+2n,\cdots\}.$$

例如,

$$\mathbf{I}_{\sim 2}=\{S_0,S_1,S_2,S_3,\cdots\},$$

$$\mathbf{I}_{\sim 5}=\{S_1,S_2,S_3,\cdots\}.$$

由于列举集合元素时,可将重复者去掉,故

$$\mathbf{I}_{\sim 2}=\{S_0,S_1\}=\{S_3,S_4\},$$

$$\mathbf{I}_{\sim 5}=\{S_0,S_1,S_2,S_3,S_4\}=\{S_5,S_{11},S_{17},S_{23},S_{34}\}.$$

表示的完全集有不同的选法.

为方便起见,通常选择一个最简明的完全集,它的根据是

引理 1 对任意 $m\in\mathbf{I}$,恒有 $q,r\in\mathbf{I}$ 使得 $m=q\cdot n+r$, $0\leqslant r<n$.而且,满足上述要求的 q,r 均由 m 唯一确定.

证明 用长除法(也称为带余除法)应有 $q,r\in\mathbf{I}$ 使得

$$m=q\cdot n+r,\quad 0\leqslant r<n.$$

现证唯一性,如果又有 $q_1,r_1\in\mathbf{I}$ 使

$$m=q_1\cdot n+r_1,\quad 0\leqslant r_1<n.$$

两式相减即得

$$(q-q_1)n=r-r_1,$$

从而 n 能整除 $r-r_1$.但 $r-r_1$ 的绝对值小于 n,若能被 n 整除,只能 $r_1-r=0$,即

$$r=r_1,$$

进而 $(q-q_1)n=0$, $q-q_1=0$, $q=q_1$. ▌

这样，上面讲的自然映射 γ，

$$\gamma: m \to S_m$$

而引理告诉我们 m 确定一个整数 r，满足

$$m = q \cdot n + r, \quad 0 \leqslant r < n.$$

于是，必有 $S_m = S_r$.

所以，我们记

$$\gamma(m) = S_r, \quad 对任意\ m \in \mathbf{I},$$

$$\mathbf{I}_{n} = \{S_0, S_1, \cdots, S_{n-1}\}$$
$$= \{[0], [1], \cdots, [n-1]\},$$

就避免了开列 $\mathbf{I}_{n}$ 元素时可能出现重复的情形. 也就是

$$\gamma(1) = [1],\ \gamma(2) = [2],\ \cdots,\ \gamma(n-1) = [n-1],$$
$$\gamma(n) = [0],\ \gamma(n+1) = [1],\ \cdots.$$

这个映射今后要不断地出现，读者必须彻底搞清楚.

由于大家在初等数学、微积分学和线性代数学中接触过大量的映射和函数实例，这里就不再多举具体例子了.

要再次提醒读者，映射 $f: A \to B$ 不要求 B 中每个元素 y 都必被 A 中某个元素 a 对应. 例如，上例中的 $2, 4 \in B$，但 a, b, c 都不对应它们.

同样，也并没要求 A 中不同元素一定对应 B 中不同元素. 例如，上例中 $f(a) = f(c) = 1$.

定义 2 设 f 是 A 到 B 的映射，称

$$\mathrm{Img}(f) = \{y \in B \mid 有\ a \in A\ 使\ y = f(a)\}$$

为映射 f 的**像**.

若 $\mathrm{Img}(f) = B$，则说 f 是**满射**或 f 是**满的**，或 f 是**映上的**.

若对任意 $a, b \in A$，$f(a) = f(b)$ 蕴涵 $a = b$，则说 f 是**单射**或 f 是**单的**，或 f 是 **1-1 的**.

当映射 f 是单射又是满射时，称之为**双射**或 f 是 **1-1 映上的**.

例 5 设 $f:\mathbf{I}\to\mathbf{I}$, f 把 n 变成 $2n$,即

$$f(n)=2n,\quad n\in\mathbf{I},$$

则 f 为单射.因为 $f(n)=f(m)$,即 $2n=2m$ 蕴涵 $n=m$.但 f 不是满射,$3\notin \mathrm{Img}(f)$.

设 $g:\mathbf{I}\to\mathbf{I}$,

$$g(n)=\begin{cases}(n+1)/2, & \text{当 } n \text{ 为奇数时},\\ n/2, & \text{当 } n \text{ 为偶数时},\end{cases}$$

则 g 为满射.因为,对任意 $m\in\mathbf{I}$,都有

$$f(2m)=m,$$

$m\in\mathrm{Img}(g)$.当然,$f(2m-1)$也等于 m,但要说明 $m\in\mathrm{Img}(g)$,只要指出有一个整数在 g 之下变成 m 就足够了.

设 $h:\mathbf{I}\to\mathbf{I}$,

$$h(n)=n+100,$$

那么,h 既是满的又是单的,从而 h 是 $\mathbf{I}$ 到 $\mathbf{I}$ 的双射.

定义 3 设 $f:A\to B$, $g:B\to C$,那么,规定,任意 $a\in A$(此 a 唯一对应 $f(a)$,而 $f(a)\in b$ 在 g 之下唯一对应 C 中元 $g(f(a))$),对应 $g(f(a))\in C$,这是 A 到 C 的映射,称为是 f 和 g 的**复合映射**,也说是 f 和 g 的**乘积**,并记为 $g\circ f$,也就是 $g\circ f:A\to C$,

$$(g\circ f)(a)=g(f(a)),\quad a\in A.$$

显然,映射 f 和映射 g 有复合映射 $g\circ f$,并不意味着 g 和 f 一定有复合映射.即使 f 和 g 能复合,g 和 f 也能复合,也未必有

$$f\circ g=g\circ f.$$

例 6 设 $A=\{x,y,z\}$, $B=\{1,2,3\}$, $C=\{a,b\}$,映射 $f:A\to B$, $g:B\to C$,且

$$f(x)=1,\quad f(y)=2,\quad f(z)=3,$$
$$g(1)=a,\quad g(2)=b,\quad g(3)=a$$

(如图 1-8).则 $g\circ f:A\to C$,且

$$(g\circ f)(x)=a,\quad (g\circ f)(y)=b,\quad (g\circ f)(z)=a.$$

对这两个映射 f,g 而言,$f\circ g$ 无意义.

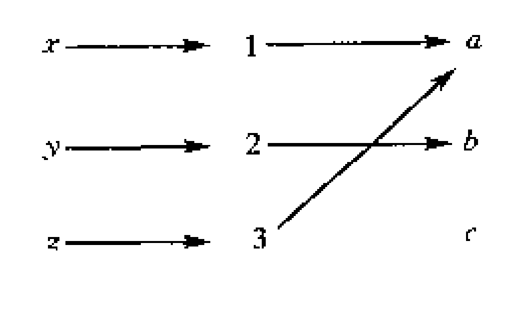


图 1－8

例 7 设 $f:\mathbf{R}\to\mathbf{R}$, $g:\mathbf{R}\to\mathbf{R}$,

$$f(x)=x^2,\quad x\in\mathbf{R},$$

$$g(x)=x+1,\quad x\in\mathbf{R}.$$

则 $f\circ g:\mathbf{R}\to\mathbf{R}$, $g\circ f:\mathbf{R}\to\mathbf{R}$,且

$$(f\circ g)(x)=(x+1)^2$$

$$=x^2+2x+1,\quad x\in\mathbf{R},$$

$$(g\circ f)(x)=x^2+1,\quad x\in\mathbf{R}.$$

要说明 $f\circ g\neq g\circ f$,只要指出,它们不是对 $\mathbf{R}$ 的每个元素 a 来说,对应的 $(g\circ f)(a)$ 与 $(f\circ g)(a)$ 恒相同,也就是要指出,至少有一个实数 a, $(f\circ g)(a)\neq(g\circ f)(a)$. 取 $a=1$,

$$(f\circ g)(1)=4,\quad (g\circ f)(1)=2,$$

即说明问题.

命题 1 设 $f:A\to B$, $g:B\to C$, $h:C\to D$. 则

$$h\circ(g\circ f)=(h\circ g)\circ f.$$

证明 首先,由 $f:A\to B$ 和 $g:B\to C$,知 $g\circ f:A\to C$,从而

$$h\circ(g\circ f):A\to D.$$

同时,由 $g:B\to C$, $h:C\to D$ 知 $h\circ g:B\to D$,进而

$$(h\circ g)\circ f:A\to D.$$

这说明 $h\circ(g\circ f)$ 和 $(h\circ g)\circ f$ 都是从 A 到 D 的映射.

进一步,对任意 $a\in A$,因为

$$(h\circ(g\circ f))(a)=h((g\circ f)(a))=h(g(f(a))),$$

$$((h\circ g)\circ f)(a)=(h\circ g)(f(a))=h(g(f(a))),$$

所以, $h\circ(g\circ f)=(h\circ g)\circ f$. ▍

这类问题的证明,有时事情本来很简单,但由于符号使用过多而掩盖了命题本身的直观性. 我们介绍一种能帮助人们直观地处理类似问题的术语.

设 $f:A\to B$, $g:B\to C$. 如果有 $k:A\to C$ 使得 $k=g\circ f$,则说,有 g 使得图 1－9 可交换.

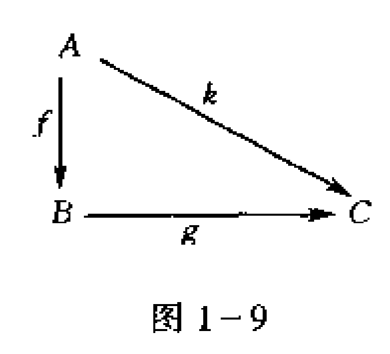


图 1－9

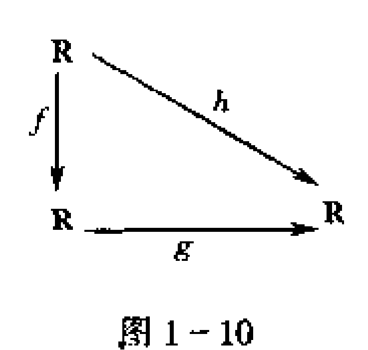
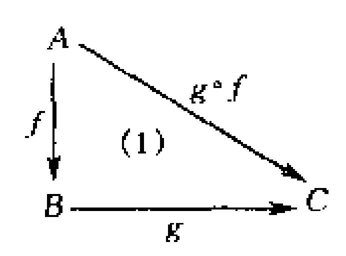


图 1－10

譬如，在例 7 中，若令 $h(x)=x^2+1$，$x\in\mathbf{R}$，则图 1－10 可交换.

命题 1 是说，对于 f,g,h，有可交换的图形



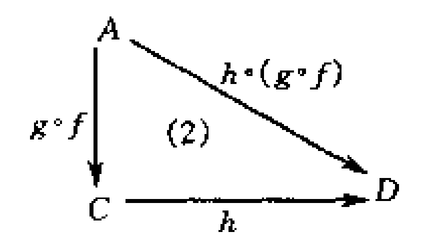
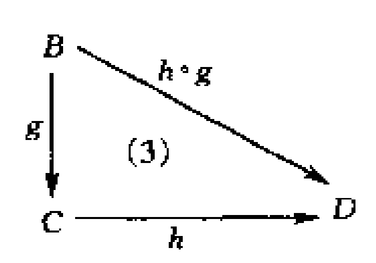


图 1－11

和可交换的图形



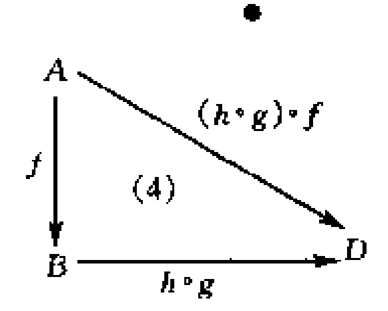


图 1－12

进一步，把三角形(4)斜边上$(h\circ g)\circ f$换成$h\circ(g\circ f)$仍为可交换图形. 当然，也可以说三角形(2)的斜边上$h\circ(g\circ f)$换成$(h\circ g)\circ f$后仍为可交换图形.

画个示意图(图 1－13)，即要求 A 中任意元素 a 经过两条不

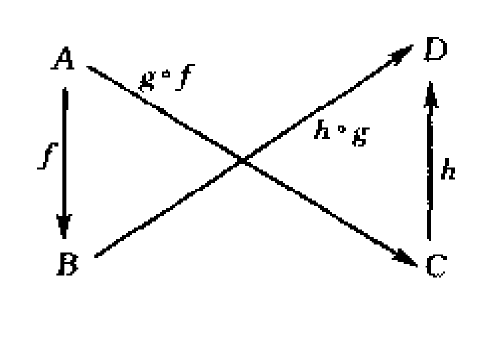


图 1－13

同的路径，变化的结果是相同的.

"图形可交换"一词已经广泛出现在很多现代数学分支中，使用起来方便而直观，特别便于初学者分辨一个元素（如 a，$f(a)$，$(g\circ f)(a)$，$(h\circ g)(b)$）究竟属于哪个集合，哪些映射是可以复合的，复合的映射是从哪里到哪里，等等.

本课不要求读者知道更复杂的可交换图形，所有这类图形，均可作为示意图理解. 甚至不理会这些图形也绝不会影响各定理的证明.

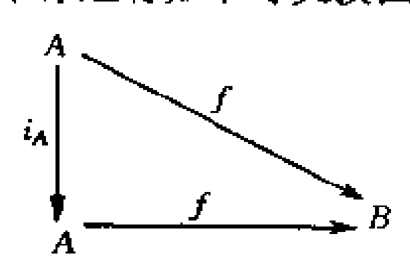
命题 2 设 $f:A\to B$，则 $f\circ i_A = i_B\circ f = f$.

证明 对任意 $a\in A$，

$$(f\circ i_A)(a) = f(i_A(a)) = f(a),$$

从而 $f\circ i_A = f$. 同理，$i_B\circ f = f$. ▌

这个命题有如下可交换图形



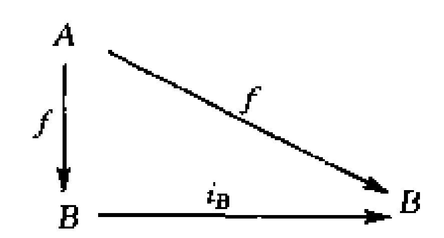


图 1－14

命题 3 设 $f:A\to B$，$g:B\to C$，那么

(1) 如果 f 和 g 都是满的，则 $g\circ f$ 亦然；

(2) 如果 f 和 g 都是单的，则 $g\circ f$ 亦然；

(3) 如果 $g\circ f$ 是满的，则 g 是满的；

(4) 如果 $g\circ f$ 是单的，则 f 是单的.

证明 假设 f 和 g 都是满的. 对任意 $c\in C$，由于 g 是满的，必有 $b\in B$，使得

$$c=g(b).$$

对于这个 b,由于 f 也是满的,从而有 $a\in A$ 使

$$b=f(a).$$

于是就有

$$c=g(b)=g(f(a))=(g\circ f)(a).$$

由 c 的任意性,知 $g\circ f$ 为满射.

假设 f 和 g 都是单射,且有 $c_1,c_2\in C$,使 $(g\circ f)(c_1)=(g\circ f)(c_2)$,即

$$g(f(c_1))=g(f(c_2)).$$

则有 $f(c_1),f(c_2)\in B$.而 g 是 B 到 C 的单射,故必有 $f(c_1)=f(c_2)$.又由于 f 是 A 到 B 的单射,条件 $f(c_1)=f(c_2)$ 就蕴涵 $c_1=c_2$.把本段证明之首尾拿出来看,就是,$(g\circ f)(c_1)=(g\circ f)(c_2)$ 蕴涵

$$c_1=c_2.$$

假设复合映射 $g\circ f$ 是满的.那么,对任意 $c\in C$,必有 $a\in A$ 使得 $(g\circ f)(a)=c$.即

$$(g\circ f)(a)=g(f(a))=c,$$

令 $b=f(a)$,则 $b\in B$,且 $g(b)=c$,由 c 的任意性知 g 为满射.

假设复合映射 $g\circ f$ 为单的,且有 $a_1,a_2\in A$ 使 $f(a_1)=f(a_2)$.那么,必有

$$(g\circ f)(a_2)=g(f(a_2))=g(f(a_1))=(g\circ f)(a_1).$$

而 $g\circ f$ 是单射,上式即意味着 $a_1=a_2$,也就是说 f 为单射. ▌

这类问题证明并不难,但当有几个映射复合在一起时,要牵涉到几个集合,必须时刻注意搞清楚,中间出现的元素是在哪个集合里.每前进一步之前,先明确下一步打算证明什么,怎样才算证明了这个事实,然后再开始论证.

定义 4 设 $f:A\to B$,说 f 是**可逆映射**,如果有 $g:B\to A$ 使得

$$g\circ f=i_A,\quad f\circ g=i_B.\qquad (*)$$

比如,例 7 中,$g:\mathbf{R}\to\mathbf{R}$,

$$g(x)=x+1,\quad x\in\mathbf{R}$$

是可逆映射,原因是有 $h:\mathbf{R}\to\mathbf{R}$,

$$h(x)=x-1,\quad x\in\mathbf{R}$$

恰好使得

$$(g\circ h)(x)=(x-1)+1=x=i_{\mathbf{R}}(x),$$
$$(h\circ g)(x)=(x+1)-1=x=i_{\mathbf{R}}(x).$$

该例中的 $f:\mathbf{R}\to\mathbf{R}$,

$$f(x)=x^2,\quad x\in\mathbf{R},$$

却不是一个可逆映射.要说明一个映射不是可逆映射,看起来是件复杂的事情,需指出,任意 $k:B\to A$ 都不能使

$$k\circ f=i_A,\quad f\circ k=i_B$$

两等式同时成立.

将来,我们会学到一些简单的判别方法.

不过,对于例 7 中的 f,大家都很熟悉,说明它不是可逆映射的这件事并不难.

对任意 $k:B\to A$,必有

$$(f\circ k)(x)=f(k(x))=(k(x))^2,\quad x\in\mathbf{R}.$$

而当 $x=-1$ 时,$k(-1)\in\mathbf{R}$,但

$$(k(-1))^2\neq-1;$$

也就是说 $(k(x))^2=x=i_{\mathbf{R}}(x)$ 不是对所有 $x\in\mathbf{R}$ 都成立.从而 $f\circ k\neq i_{\mathbf{R}}$.$f$ 不是可逆映射.

下面,先给出一个判别映射是否可逆的充分必要条件.

定理 2 映射 $f:A\to B$ 是可逆的,必要而只要,f 是双射.

证明 如果 f 是可逆映射,那么,应有映射 $g:B\to A$ 使得

$$g\circ f=i_A,\quad f\circ g=i_B.$$

由于恒等映射 i_A 是单的,据命题 3 之(4)款,f 必然是单射.又由

于恒等映射 i_B 是满的，据命题 3 之(3)款，f 必然是满射. 所以，f 是双射.

反过来，如果 $f: A \to B$ 是个双射，我们来确定 B 到 A 的一个映射 g 使得(*)成立.

对任意 $b \in B$，由于 f 为满射，故必有 $a \in A$ 使 $f(a) = b$. 而且，由于 f 是单射，不能有另外的 A 中元素在 f 之下也变成 b. 这就是说，按这种办法，我们确定了一个规则，B 中的每一个元素 b 都有而且只有一个 $a \in A$ 与之对应. 这个规则(也就是 B 到 A 的一个映射)记为 g，则 $g: B \to A$，对任意 $b \in B$，

$$g(b) = a, \quad f(a) = b.$$

再来验证(*). 对任意 $b \in B$，设 $f(a) = b$，则

$$(f \circ g)(b) = f(g(b)) = f(a) = b = i_B(b),$$

也就是 $f \circ g = i_B$.

同样，对任意 $a \in A$，设 $f(a) = b$，那么，按 g 的定义，应有 $g(b) = a$，于是

$$(g \circ f)(a) = g(f(a)) = g(b) = a = i_A(a). \qquad \blacksquare$$

命题 4 设 $f: A \to B$ 是可逆映射. 那么，使得

$$f \circ g = i_B, \quad g \circ f = i_A$$

的 $g: B \to A$ 是由 f 唯一确定的(此时记 $g = f^{-1}$).

证明 如果还有 $h: B \to A$ 使

$$f \circ h = i_B, \quad h \circ f = i_A,$$

那么，由命题 1 知$(g \circ f) \circ h = g \circ (f \circ h)$，但

$$(g \circ f) \circ h = i_A \circ h = h, \quad g \circ (f \circ h) = g \circ i_B = g,$$

从而 $h = g$. $\blacksquare$

当 $f: A \to B$ 可逆时，这个由 f 唯一确定的映射 $f^{-1}: B \to A$ 即称之为 f 的**逆映射**.

关于映射，还有一个常用记号：设 f 是集合 A 到集合 B 的任意一个映射，S 是 A 的一个子集. 则将 B 的子集

$$f(S)=\{y\in B \mid 有\ x\in S\ 使\ y=f(x)\}$$

称为 S 在 f 之下的像.

前已定义,映射 f 是满的,当而且只当,$f(A)=B$.

对 B 的任意子集 T,称 A 的子集

$$\{x\in A \mid f(x)\in T\}$$

为 T 在 f 之下的原像,记为 $f^{-1}(T)$. 这里加 -1 绝不意味着 f 可逆,对一般映射 f 及 B 的每个子集 S,$f^{-1}(S)$都有意义. 如例 7 中,$f:\mathbf{R}\to\mathbf{R}$ 并不是双射. 取$\{4,9\}\subseteq\mathbf{R}$,则

$$f^{-1}(\{4,9\})=\{-2,2,-3,3\}.$$

映射 $f:A\to B$ 是个对应规则,它当然使 A 中子集 S 的每个元素 s 对应 B 中元素 $f(s)$,这就诱导出 S 到 B 的映射,通常记为 $f|_S$. 对任意 $s\in S$,有 $f|_S(s)=f(s)$.

注意,f 是 A 到 B 的映射,$f|_S$ 是 S 到 B 的映射. 它们的关系是:限制在子集 S 上看,这两个映射的效果是一样的. 也可记为:

命题 5 设 $f:A\to B$, S 是 A 的子集,则 $f|_S=f\circ i_B$,也就是下图形可交换.

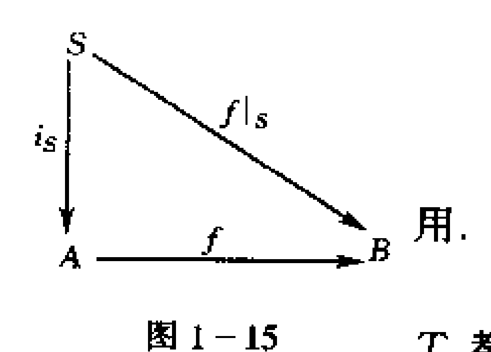


图 1-15

事实上,对任意 $s\in S$,我们有

$$(f\circ i_S)(s)=f(i_S(s))=f(s). \quad \blacksquare$$

下面这个命题在以后各章中要经常引用.

命题 6 设 $f:A\to B$,对 B 的任意子集 T,都有

$$f(f^{-1}(T))=T\cap \mathrm{Img}(f).$$

证明 若 $y\in T\cap\mathrm{Img}(f)$,即 $y\in T$. 而且 $y\in\mathrm{Img}(f)$,从而必有 $x\in A$,使得

$$y=f(x).$$

于是知 $f(x)=y\in T$, $x\in f^{-1}(T)$. 故

$$f(x)\subseteq f(f^{-1}(T)).$$

但 $f(x)$就是 y,所以知 $y\in f(f^{-1}(T))$. 也就是

$$T\cap \mathrm{Img}(f)\subseteq f(f^{-1}(T)).$$

反过来,如果 $z\in f(f^{-1}(T))$,则有 $u\in f^{-1}(T)$使

$$z=f(u),$$

故 $z\in \mathrm{Img}(f)$. 而 $u\in f^{-1}(T)$这件事意味着

$$f(u)\in T,$$

这个 $f(u)$就是 z,即 $z\in T$. 合起来,$z\in T\cap \mathrm{Img}(f)$,从而

$$f(f^{-1}(T))\subseteq T\cap \mathrm{Img}(f).$$

所以,$f(f^{-1}(T))=T\cap \mathrm{Img}(f)$. ▌

学好本节的关键是弄懂"映射"、"可逆映射"的定义. 我们通过例子把这些概念串一串.

设 $f:A\to B$ 是 A 到 B 的映射,通常,称 A 为 B 的**定义域**,B 为 f 的**值域**.

不能脱离定义域和值域来谈映射. 让我们讨论下列问题.

1. $A=\{(x,y)\mid x^2+y^2\leqslant 1\}$是映射关系吗?

答:提法不对,没有定义域和值域.

2. $A=\{(x,y)\in \mathbf{R}\times\mathbf{R}\mid x^2+y^2\leqslant 1\}$是个映射关系吗?

答:A 给出了 $\mathbf{R}$ 上的一个关系. 但当 $x=2$ 时,对任意 $y\in\mathbf{R}$,恒有

$$2^2+y^2>1.$$

即没有任何 $y\in\mathbf{R}$ 使$(2,y)\in A$,使 2 与 y 有 A 关系,故 A 不是映射关系.

3. 用 K 代表

$$\{x\in\mathbf{R}\mid -1\leqslant x\leqslant 1\},$$

那么,$A=\{(x,y)\in K\times\mathbf{R}\mid x^2+y^2\leqslant 1\}$是个映射关系吗?

答:A 确定 $K\times\mathbf{R}$ 上一个关系,但不是映射关系.

当 $x=0$ 时,每个 z, $-1\leqslant z\leqslant 1$ 都满足

$$0^2+y^2\leqslant 1,$$

而映射关系要求"对每个 $x\in K$ 都要有唯一确定的 $y\in\mathbf{R}$ 使$(x,y)\in A$".

4. $A=\{(x,y)\in K\times\mathbf{R}\mid x^2+y^2=1\}$是个映射关系吗?

答:仍然不是.因为,对 $x=0$,有$(0,1)\in A$,$(0,-1)\in A$.

5. 用 J 代表集合

$$\{z\in\mathbf{R}\mid 0\leqslant z\leqslant 4\},$$

那么,$A=\{(x,y)\in K\times J\mid x^2+y^2=1\}$是 $K\times J$ 的一个映射关系吗?

答:是.因为,对每个 $x\in K$ 都有J 中一个唯一确定的y 使得

$$(x,y)\in A.$$

6. 用 H 代表集合

$$\left\{z\in\mathbf{R}\,\middle|\,-\frac{1}{2}\leqslant z\leqslant 0\text{或}\frac{1}{2}<z<100\right\},$$

那么,$A=\{(x,y)\in K\times H\mid x^2+y^2=1\}$是 $K\times H$ 的一个映射关系吗?

答:是.

7. 上问中的 H 换成

$$M=\left\{z\in\mathbf{R}\,\middle|\,-\frac{1}{2}\leqslant z\leqslant 0\text{或}\frac{1}{2}\leqslant z<100\right\},$$

$$N=\left\{z\in\mathbf{R}\,\middle|\,-\frac{1}{2}<z\leqslant 0\text{或}\frac{1}{2}<z<80\right\},$$

$$L=\left\{z\in\mathbf{R}\,\middle|\,-\frac{1}{2}<z\leqslant 0\text{或}\frac{1}{2}\leqslant z<60\right\},$$

情况会发生怎样的变化?

答:$A=\{(x,y)\in K\times M\mid x^2+y^2=1\}$不是映射关系,因为

$$\left(\sqrt{\frac{3}{4}},\frac{1}{2}\right)\in A,\quad\left(\sqrt{\frac{3}{4}},-\frac{1}{2}\right)\in A,$$

即 K 中数$\sqrt{3}/2$ 在 A 的元素中出现了两次.

而 $B=\{(x,y)\in K\times M\mid x^2+y^2=1\}$也不是映射关系,因为$\sqrt{3}/2\in K$,但没有 N 中元素 y 使

$$(\sqrt{3}/2,y)\in B.$$

但是，$C=\{(x,y)\in K\times L\mid x^2+y^2=1\}$是个映射关系.

8. 上面第 5 问中 A 所确定的映射 $f: K\to J$，$(x,f(x))\in A$，是个满射吗？

答：f 不是满的，因为没有任何 $x\in K$ 使$(x,4)\in A$，即对任何 $x\in K$ 恒有$f(x)\neq 4$，$4\notin \operatorname{Img}(f)$.

9. 令 $P=\{z\in\mathbf{R}\mid 0\leqslant z\leqslant 1\}$. 那么，

$$A=\{(x,y)\in K\times P\mid x^2+y^2=1\}$$

确定的 K 到 P 的映射是满的吗？是单的吗？

答：是个满射. 因为，对每个 $b\in P$，即

$$0\leqslant b\leqslant 1$$

必有 $a=\sqrt{1-b^2}\in K$，使得$(a,b)\in A$.

但，它不是单的，因为$(-1,0)\in A$，$(1,0)\in A$.

10. 用元素对应法给出问 9 中确定的映射.

答：由问 9 的映射关系得映射 $f: K\to P$，

$$y=f(x)=\sqrt{1-x^2}.$$

它不是单射，因为 $f(1)=f(-1)=0$.

11. 给出 $\mathbf{R}$ 的子集 X,Y，使得$\{(x,y)\in X\times Y\mid x^2+y^2=1\}$确定 X 到 Y 的双射.

答：可以给出很多. 例如，

$$X_1=K,\quad Y_1=K,$$

$$A_1=\{(x,y)\in K\times K\mid x^2+y^2=1 \text{ 且 } xy\geqslant 0\};$$

$$A_2=\{(x,y)\in K\times K\mid x^2+y^2=1 \text{ 且 } xy\leqslant 0\};$$

$$X_2=P,\quad Y_2=P,$$

$$A_3=\{(x,y)\in P\times P\mid x^2+y^2=1\};$$

$$X_3=\left\{x\in\mathbf{R}\,\middle|\,\frac{1}{2}\leqslant x\leqslant 1 \text{ 或 } -\frac{1}{2}<x\leqslant 0\right\},$$

$$Y_3=\left\{y\in\mathbf{R}\,\middle|\,-\frac{\sqrt{3}}{2}<y\leqslant\frac{\sqrt{3}}{2}\right\},$$

$$A_4=\{(x,y)\in X_3\times Y_3\mid x^2+y^2=1,\ xy\geqslant 0\}.$$

可画示意图如图 1－16.

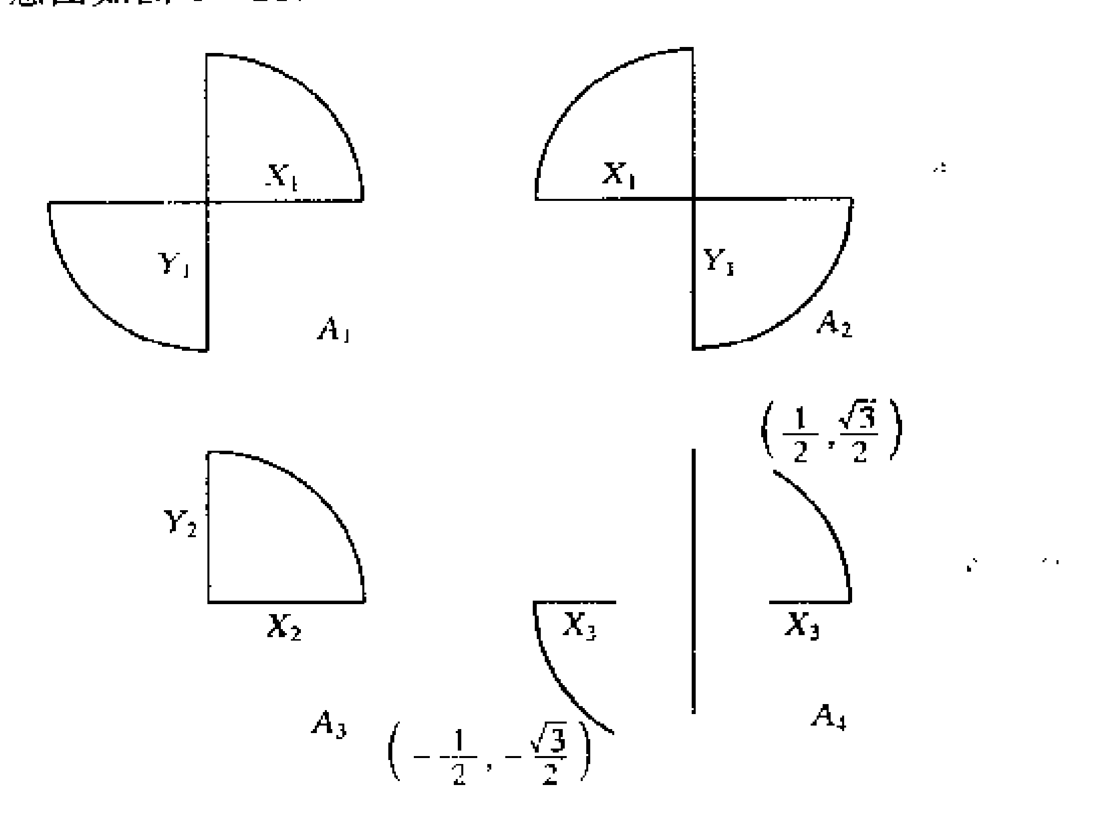


图 1－16

12． 用元素对应方式给出 11 款中 A_3 和 A_4 所确定的映射.

答：由 A_3 确定的映射记为 f，A_4 确定的映射记为 g，则有

$$f:P\to P,\quad g:X_3\to Y_3,$$

$$y=f(x)=\sqrt{1-x^2},$$

$$y=g(x)=\begin{cases}\sqrt{1-x^2}, & \text{当}\frac{1}{2}\leqslant x\leqslant 1\text{时},\\ -\sqrt{1-x^2}, & \text{当}-\frac{1}{2}<x\leqslant 0\text{时}.\end{cases}$$

13． 给出上述映射 f 和 g 的逆映射.

答：由于 f 和 g 都是双射，所以它们都有逆映射.

$$f^{-1}:P\to P,\quad g^{-1}:Y_3\to X_3,$$

$$x=f^{-1}(y)=\sqrt{1-y^2},$$

$$x=g^{-1}(y)=\begin{cases}\sqrt{1-y^2}, & \text{当 } 0\leqslant y\leqslant\frac{\sqrt{3}}{2}\text{ 时},\\ -\sqrt{1-y^2}, & \text{当 } -\frac{\sqrt{3}}{2}<y<0\text{ 时}.\end{cases}$$

习　题　四

1. 条件如例 7,给出映射 $f\circ f, g\circ g$ 和 $(g\circ f)\circ g, (f\circ g)\circ f$.

2. 给出一个例子,$f:A\to B, g:B\to C$ 使得 $g\circ f$ 是单射,但 g 并不是单射.

3. 设 $f:A\to B$, $g:A\to B$, $h:B\to C$. 如果 h 是单射,则 $h\circ f=h\circ g$ 蕴涵

$$f=g.$$

4. 设 $h:A\to B$, $g:B\to C$, $f:B\to C$. 如果 h 是满射,则 $f\circ h=g\circ h$ 蕴涵

$$f=g.$$

5. 如果 $f:A\to B$ 和 $g:B\to C$ 都是可逆映射,则 $g\circ f:A\to C$ 是可逆映射,而且

$$(g\circ f)^{-1}=f^{-1}\circ g^{-1}.$$

6. 给定实数 a,b,用它们确定 $\mathbf{R}$ 到 $\mathbf{R}$ 的一个映射 f,规定

$$f(x)=ax+b.$$

问,何时 f 为单射,何时为满射.

7. 设 $f:A\to B$, $S_1,S_2\subseteq A$. 证明:

$$f(S_1\cap S_2)\subseteq f(S_1)\cap f(S_2),\quad f(S_1)\cup f(S_2)=f(S_1\cup S_2).$$

8*. 设 $f:A\to B$, $g:B\to C$. 证明: $\mathrm{Img}(g\circ f)=g(\mathrm{Img}(f))$.

§5　置　　换

只含有限个元素的集合称之为有限集. 非空的有限集 A 到 A 本身的可逆映射称之为 A 上置换,也就是 A 的一个置换.

由于 n 元集的元素可用自然数标号,记为

$$a_1, a_2, \cdots, a_n,$$

一个置换将 a_i 变成a_j，即把 A 的第 i 个元变成第 j 个元，可以简单说把 i 变到 j，而不引起混乱. 如果需要的话，在讨论问题时，可以把每个 a_i 的a 省去，只记为 i，最后再把各相应的 i 再填上 a 记为 a_i 就行了.

也就是说，我们只要讨论集合

$$\mathbf{S} = \{1, 2, \cdots, n\}$$

上的置换，则任意 n 元集上的置换就有办法处理了.

设 $\mathbf{S} = \{1,2,3\}$. 对于 $\mathbf{S}$ 上的一个置换 P，可列一表，记成

$$P = \begin{pmatrix} 1 & 2 & 3 \\ P(1) & P(2) & P(3) \end{pmatrix},$$

即把每个数字在 P 之下对应的那个数字记在它的下方. 于是 $\mathbf{S}$ 上有六个不同的置换，它们是

$$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

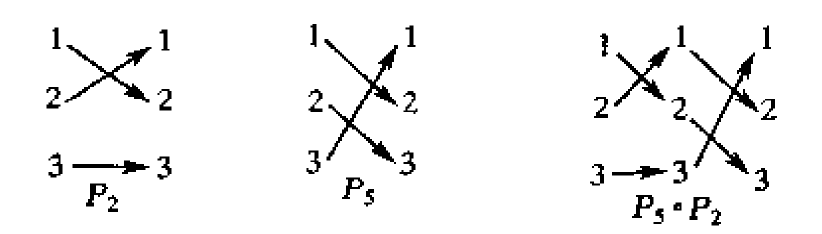
$$P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

当然，也可以把 P_1 写成

$$\begin{pmatrix} 3 & 2 & 1 \\ 3 & 2 & 1 \end{pmatrix},$$

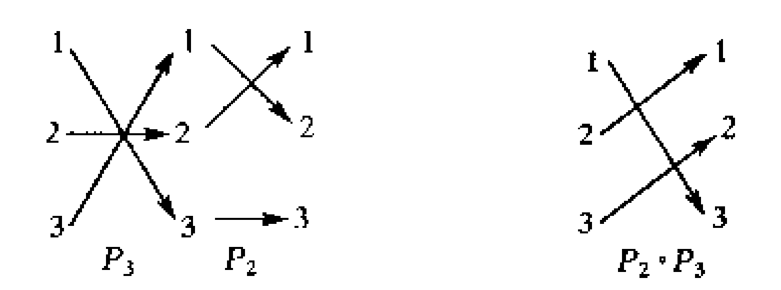
等等. 因为，作为映射，效果相同者即为相等映射.

可以用很直观的办法来计算两个置换的复合. 例如



把相连的射线接起来看，即知 $P_5 \circ P_2 = P_3$.

也就是，把要进行复合的映射的图连起来，把结果记下来，即得其复合. 如



下面研究一般情形，设

$$\mathbf{S} = \{1, 2, \cdots, n\}.$$

命题 1 S 上有 $n!$ 个不同的置换.

事实上，我们记置换的表中，上面一排取成 $1, 2, \cdots, n$，那么，下面一排，这 n 个数有 $n!$ 个排列方法. ▌

定义 1 数码 $1, 2, \cdots, n$ 的每一个有确定次序的排列称为一个 n 排列. 在一个 n 排列中，如果有较大的数排在较小的数之前，则说这两个数构成一个**反序**，该排列中出现的反序的个数称为是它的**反序数**.

例如，下面的 1,2,3,4 排列中出现反序情况是

排列	反序	反序数
1,2,3,4	无	0
1,4,3,2	(4,3),(4,2),(3,2)	3
2,3,1,4	(2,1),(3,1)	2
4,2,3,1	(4,1),(4,2),(4,3),(2,1),(3,1)	5

命题 2 若把一个 n 排列中某相邻两数码互换位置，则所得到的新排列的反序数与原排列的反序数差 1.

事实上，设所考虑的排列为

$$\cdots, i, j, \cdots, \qquad (*)$$

调换后，得新排列

$$\cdots,j,i,\cdots,$$

看(*)的任意反序(k,l).如果k,l既不是i也不是j,此次调换后,k和l没动,(k,l)仍为反序.如果l是i,j中一个,而k不是,那么,这次调动l仍然在k的后面,(k,l)仍为反序.同理,若k为i,j中一个,而l不是,那么(k,l)仍为反序.对于不是反序者可同样说明.

剩下的只需看i和j两个数码了.如果在原排列中(i,j)是反序,新排列中就不是了;如果在原排列中i和j不是反序,那么新排列中(i,j)为反序.

总而言之,两个排列间仅差一个反序. ▌

命题3 当$n>1$时,$n!$个n排列中,反序数为偶数者恰有一半,即$n!/2$个.

证明 设所有反序数为偶数的排列作成的集合为A,所有反序数为奇数的排列作成的集合为B.

建立A到B的映射σ,规定A中元

$$i,j,k,l,\cdots \tag{1}$$

对应B中元

$$j,i,k,l,\cdots, \tag{2}$$

其中k,l以后各数码在两排列中顺序相同.命题2已经证明前者反序数为偶数时,后者之反序数为奇数,这个对应确为A到B的映射.它把A中序列前两数码换位后得B中数列,显然σ是个单射.

又,B中每个排列(2),前两数码对调后必得A中排列(1),这个排列在规定的映射下,恰好对应B中排列(2);也就是说,这个映射σ是双射.从而A和B有相同多的元素,各为$n!/2$. ▌

命题4 将一n排列之两数码(未必相邻)对调,得到的新排列与原排列的反序数奇偶性相反.

证明 我们只证明原排列反序数为偶数时,对调两数码后的新排列之反序数必为奇数.另外的情形可对偶地得到证明.

设有排列

$$\cdots,i,j_1,\cdots,j_t,k,\cdots, \tag{3}$$

在 i 和 j 中间有 t 个数码. 对调 i 和 j,得

$$\cdots,k,j_1,\cdots,j_t,i,\cdots \tag{4}$$

如果(3)之反序数为偶数,据命题 3,将 i 和 j_1 对调,余者不动,新排列

$$\cdots,j_1,i,j_2,\cdots,j_t,k,\cdots$$

的反序数必为奇数. 再对换 j_2 和 i……得新排列

$$\cdots,j_1,\cdots,j_t,i,k,\cdots, \tag{5}$$

其反序数奇偶性变了 t 次. 再对换 i 和 k,得

$$\cdots,j_1,\cdots,j_t,k,i,\cdots.$$

继续对调 j_t 与 k……j_1 与 k,得

$$\cdots,k,j_1,\cdots,j_t,i,\cdots. \tag{6}$$

从(5)到(6),反序数的奇偶性又变化了 $1+t$ 次.

总起来,从(3)到(6),两排列之反序数的奇偶性变化了 $2t+1$ 次,(3)的反序数为偶数,则(6)的反序数必为奇数. ▌

定义 2 设 P 是$\{1,2,\cdots,n\}$上的一个置换,记

$$P=\begin{pmatrix} 1 & 2 & \cdots & n \\ P(1) & P(2) & \cdots & P(n) \end{pmatrix}.$$

当排列 $P(1),P(2),\cdots,P(n)$的反序数为偶数时,称 P 为**偶置换**,否则即称为**奇置换**.

命题 5 偶置换 P 用任意方式给出

$$P=\begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ P(i_1) & P(i_2) & \cdots & P(i_n) \end{pmatrix}, \tag{\#}$$

其上下两排排列的反序数之差恒为偶数,若 P 为奇置换,则任意一个 n 排列

$$i_1,i_2,\cdots,i_n \tag{7}$$

的反序数与

$$P(i_1), P(i_2), \cdots, P(i_n) \tag{8}$$

的反序数之差恒为奇数.

证明 在排列(7)中对调 i_1 和某个 $i_k=1$,新的排列变奇偶性一次.相应地,在(8)中对调 $P(i_1)$和 $P(i_k)$得新排列,奇偶性亦变一次.

两个新排列排在一起,仍然是置换 P.而新表法的两排列反序数之差与原表法两排列的反序数之差奇偶性相同.

继续下去,得

$$P=\begin{pmatrix} 1 & 2 & \cdots & n \\ P(1) & P(2) & \cdots & P(n) \end{pmatrix},$$

其对应的两排列反序数之差的奇偶性与(#)表示中对应的两排列的反序数之差的奇偶性相同.所以,P 为偶置换时,排列(7)的反序数与排列(8)的反序数之差为偶数.P 为奇置换时,(7)反序数与(8)的反序数之差为奇数. ∎

命题 6 两个奇偶性相同的置换复合后为偶置换,两个奇偶性相反的置换复合后为奇置换.

证明 设 P,Q 是 $\mathbf{S}$ 上两个置换.我们只需证明,若 Q 为偶置换,则 $Q\circ P$ 和 P 奇偶性相同;若 Q 为奇置换,则 $Q\circ P$ 和 P 奇偶性相反.

Q 可以用任意方式给出,当然可记为

$$Q=\begin{pmatrix} P(1) & P(2) & \cdots & P(n) \\ Q(P(1)) & Q(P(2)) & \cdots & Q(P(n)) \end{pmatrix}.$$

且由于

$$(Q\circ P)(1)=Q(P(1)),\ \cdots,\ (Q\circ P)(n)=Q(P(n)).$$

就有

$$Q\circ P=\begin{pmatrix} 1 & 2 & \cdots & n \\ Q(P(1)) & Q(P(2)) & \cdots & Q(P(n)) \end{pmatrix}. \tag{9}$$

当 Q 为偶置换时,据命题 5,排列

$$P(1), P(2), \cdots, P(n) \tag{10}$$

的反序数与排列

$$Q(P(1)),Q(P(2)),\cdots,Q(P(n)) \tag{11}$$

的反序数奇偶性相同.从而,由定义2,知

$$P=\begin{pmatrix}1 & 2 & \cdots & n\\ P(1) & P(2) & \cdots & P(n)\end{pmatrix} \tag{12}$$

的奇偶性与(9)中的 $Q\circ P$ 的奇偶性相同.

当 Q 为奇置换时,据命题5,排列(10)的反序数与排列(11)的反序数的奇偶性相反,从而,置换(9)与置换(12)奇偶性相反. ▌

命题7 置换 P 的逆映射(在此处称为逆置换)P^{-1}与 P 的奇偶性相同.

证明 把 P 表成(12)形式,容易看出,置换

$$Q=\begin{pmatrix}P(1) & P(2) & \cdots & P(n)\\ 1 & 2 & \cdots & n\end{pmatrix} \tag{13}$$

恰为 P 之逆置换 P^{-1}.

Q 的上下两排列反序数之差就等于上排列

$$P(1),P(2),\cdots,P(n)$$

的反序数 t.由命题5, t 的奇偶性与 Q 的奇偶性相同.由定义2, t 的奇偶性就是 P 的奇偶性.所以,P 和 Q 之奇偶性相同. ▌

习 题 五

1. 求下列诸排列的反序数:

(a) $n,n-1,\cdots,2,1$;

(b) $1,3,\cdots,2n-1,2,4,\cdots,n$.

2. 对于$\{1,2,3\}$上的置换,计算 $P_2\circ P_5$,$P_5\circ P_2$,$P_3\circ P_4$ 和 $P_4\circ P_3$.

3. 给出置换

$$\begin{pmatrix}1 & 5 & 4 & 3 & 2 & 6\\ 2 & 4 & 3 & 6 & 1 & 5\end{pmatrix}$$

的逆置换.

4*. 设

$$P=\begin{pmatrix}1 & 2 & 3 & \cdots & n-1 & n\\ 2 & 3 & 4 & \cdots & n & 1\end{pmatrix}.$$

证明：$P, P\circ P, \cdots, \underbrace{((P\circ P)\circ\cdots\circ P)\circ P}_{n\text{个}}$是两两不同的置换.

§6 运　　算

从小学时代开始，人们就不断地进行各种"运算"，如整数加整数、有理数乘有理数. 到了中学阶段，进一步知道函数加函数、多项式乘多项式，等等.

在这众多的"运算"中有哪些东西本质上是相同的呢？哪些性质是由更基本的性质派生出来的呢？

在《抽象代数》中，所说的运算是以千差万别的集合为对象的，不只限于数的运算而已.

定义 1　设 S 是个非空集合，把 $S\times S$ 到 S 的映射称之为 S 上的**二元运算**，简称为 S 上**运算**.

例 1　在 $\mathbf{I}$ 上，规定任意$(m,n)\in\mathbf{I}\times\mathbf{I}$对应整数 mn，此映射即大家熟悉的整数乘法.

例 2　在所有实的 $n\times n$ 矩阵的集合 $M_{n\times n}$ 上规定，任意$(A,B)\in M_{n\times n}\times M_{n\times n}$恒对应 $n\times n$ 矩阵 AB，即得矩阵的乘法运算. 对任意$(A,B)\in M_{n\times n}\times M_{n\times n}$，规定，对应 $A+B-AB$，也得到 $M_{n\times n}$ 的一个运算.

例 3　在自然数集 $\mathbf{N}$ 上，规定(m,n)对应 m^n，也是 $\mathbf{N}$ 上的运算.

如果有人说，规定(m,n)对应 $m-n$，那么，这不符合运算定义，这不是 $\mathbf{N}\times\mathbf{N}$ 到 $\mathbf{N}$ 的映射，(2,3)在 $\mathbf{N}$ 中不知对应何物.

例 4　在 $\mathbf{I}$ 上规定，任意(m,n)对应整数 $m-n$，则得 $\mathbf{I}$ 上一运算.

在 $\mathbf{R}$ 上规定，任意$(m,n)\in\mathbf{R}\times\mathbf{R}$ 对应实数 m/n……. 该规

定，当 $n=0$ 时，是无法实现的事，这不能确定 $\mathbf{R}\times\mathbf{R}$ 到 $\mathbf{R}$ 的映射，也谈不上运算之事.

例 5 设 A 是个非空集合，$M(A)$ 是所有 $A\to A$ 的映射. 规定，对任意 $(g,f)\in M(A)\times M(A)$，也就是 $f:A\to A$ 和 $g:A\to A$，对应 f 和 g 的复合映射 $g\circ f\in M(A)$，得到集合 $M(A)$ 上一个运算.

进一步，用 $I(A)$ 代表所有 A 到 A 的可逆映射的集合. 对任意 $(g,f)\in I(A)\times I(A)$，由 §4 命题 3 可知，它们的复合 $g\circ f$ 亦为双射，也就是可逆，即 $g\circ f\in I(A)$. 规定 (g,f) 对应 $g\circ f$，得到 $I(A)$ 上一个运算.

特别地，$A=\{1,2,\cdots,n\}$，上述办法得到所有 n 阶置换的集合上的一个运算.

对于集合 S 上的运算 θ. 我们可以用 $a,b\in S$ 来代替 $(a,b)\in S\times S$ 这样的说法，当然 a,b 是有顺序的，即先说 a 后说 b，与先说 b 再说 a 是不一样的. 同时，可以把映射 θ 写到中间，即

$$\theta((a,b))=a\theta b.$$

比如，例 1 的映射记为 $\times$，也就是

$$m\times n=mn.$$

例 3 中的运算可记为 $m\odot n=m^n$.

例 6 对于有限集，可以把它上面的运算用一个表来指明.

如 $S=\{a,b\}$，表

θ	a	b
a	a	b
b	b	a

和

θ	b	a
b	a	b
a	b	a

表示

$$a\theta a=a,\ a\theta b=b,\ b\theta a=b,\ b\theta b=a.$$

这种表称为**运算表**. 竖列中的每个元与横行中每个元所对应的元素记在它们相对的交叉路口.

例 7 设 A 是一个集合，S 是 A 的幂集即 S 是 A 的所有子集

的集合. 规定$(U,V)\in S\times S$,也就是$U,V\in S$,换言之$U,V\subseteq A$,对应它们的并集$U\cup V$,则得S上一运算. 同理,规定$U,V\in S$对应它们的交集$U\cap V$,也得S上一个运算.

例 8 设$\mathbf{R}_2$是实平面上所有向量的集合. 规定,任意$\boldsymbol{u},\boldsymbol{v}\in\mathbf{R}_2$,对应$\boldsymbol{u}$和$\boldsymbol{v}$按平行四边形法则合成的那个向量$\boldsymbol{u}+\boldsymbol{v}$. 这是$\mathbf{R}_2$上的一个运算.

例 9 对一个给定的正整数n,$\mathbf{I}_n$表示一个有n个元素的集合,它的元素用0到$n-1$个数字加上*来表示,即

$$\mathbf{I}_n=\{0^*,1^*,2^*,\cdots,(n-1)^*\}.$$

我们知道,对任意整数m,作除法,必有$q,r\in\mathbf{I}$使得

$$m=qn+r,\quad 0\leqslant r<n$$

而且q,r均由m,n唯一确定(若又有q_1,r_1满足上述要求,则$(q_1-q)n=r-r_1$,由$n|(r_1-r)$知$r_1-r=0$, $r_1=r$, $q_1=q$).

对任意$i^*,j^*\in\mathbf{I}_n$,其中i,j是小于n的非负整数,作除法,可确定唯一的r满足

$$i+j=qn+r,\quad 0\leqslant r<n \tag{1}$$

规定$(i^*,j^*)\in\mathbf{I}_n\times\mathbf{I}_n$对应(1)中得到的$r$加*,即$(i^*,j^*)$对应$r^*$. 由于$0\leqslant r<n$,$r^*$是$\mathbf{I}_n$中确定的元素.

这就得到$\mathbf{I}_n$上一个运算,称为加法. 记$+(i^*,j^*)=r^*$或者

$$i^*+j^*=r^*.$$

以$\mathbf{I}_6$为例,其运算表是

+	0^*	1^*	2^*	3^*	4^*	5^*
0^*	0^*	1^*	2^*	3^*	4^*	5^*
1^*	1^*	2^*	3^*	4^*	5^*	0^*
2^*	2^*	3^*	4^*	5^*	0^*	1^*
3^*	3^*	4^*	5^*	0^*	1^*	2^*
4^*	4^*	5^*	0^*	1^*	2^*	3^*
5^*	5^*	0^*	1^*	2^*	3^*	4^*

同样道理，对任意 $0 \leqslant i, j < n$，作除法，可得唯一的 q, r 使

$$i \cdot j = qn + r, \quad 0 \leqslant r < n.$$

我们规定，任意 $i^*, j^* \in \mathbf{I}_n$，对应上法唯一确定的这个 r 加上 $*$，即

$$\theta(i^*, j^*) = r^*,$$

这是 $\mathbf{I}_n \times \mathbf{I}_n$ 到 $\mathbf{I}_n$ 的映射，θ 是 $\mathbf{I}_n$ 上的一个运算，记 $\theta(i^*, j^*)$ 为 $i^* \times j^*$，并称之为 $\mathbf{I}_n$ 上的乘法，即 $i^* \times j^* = r^*$. 这个运算所对应的表是（仍以 $\mathbf{I}_6$ 作为例子）

$\times$	0^*	1^*	2^*	3^*	4^*	5^*
0^*	0^*	0^*	0^*	0^*	0^*	0^*
1^*	0^*	1^*	2^*	3^*	4^*	5^*
2^*	0^*	2^*	4^*	0^*	2^*	4^*
3^*	0^*	3^*	0^*	3^*	0^*	3^*
4^*	0^*	4^*	2^*	0^*	4^*	2^*
5^*	0^*	5^*	4^*	3^*	2^*	1^*.

这个例中两种运算具有一定的典型意义，读者应很好地掌握.

为了进一步了解 $\mathbf{I}_n$，我们给出一个关于整数性质的引理.

一个整数 a 可以表成 $a = bc$，其中 b 和 c 都是整数，则说 b 和 c 是 a 的因子，或说它们能整除 a，记为 $b \mid a$, $c \mid a$.

如果整数 p 不等于 $0, -1, 1$ 且它只有因子 $1, -1, p$ 和 $-p$，则称 p 为素数.

所谓两个整数 a, b 的最高公因子 d 是有下条性质的一个正整数：

(1) d 是 a 的因子也是 b 的因子；

(2) 如果整数 c 是 a 的因子，又是 b 的因子，则 $c \mid d$.

最高公因子亦称最大公因子.

引理 1 任意两个非零整数 a, b 恒有最高公因子 d，且必有 $s, t \in \mathbf{I}$ 使 $d = sa + tb$.

证明 设

$$D=\{z\in\mathbf{I}\mid z=xa+yb,\ x,y\in\mathbf{I}\}.$$

D 中必含正数,比如说,若 $ka+b<0$,则必有

$$(-k)a+(-1)b>0.$$

设 $i_1\in D$, $i_1>0$,看 D 中是否有 i_2 使

$$i_1>i_2>0.$$

再看 D 中是否有 i_3 使得

$$i_2>i_3>0.$$

由于 i_1 是一个正整数,这样找下去,最后总要有 $d\in D$, $d>0$, D 中任何正整数都不小于 d. 但 $i\in D$ 意味着有 $s,t\in\mathbf{I}$,

$$d=sa+tb.$$

现在来证明 d 是 a,b 的最高公因子.

首先,作除法,有

$$a=dq+r,\quad 0\leqslant r<d.$$

从而有

$$r=a-dq=a-(sa+tb)q=(1-sq)a+(-tq)b,$$

这说明 $r\in D$, $r\geqslant 0$. 倘若 $r>0$,则与 d 的取法矛盾. 故 $r=0$, $d\mid a$. 同理 $d\mid b$.

其次,对于 a 和 b 的任意一个公因子 c,由于 $c\mid a$, $c\mid b$,进而 $c\mid(sa)$, $c\mid(tb)$. 故

$$c\mid(sa+tb)=d.$$

而 $sa+tb=d$,所以 $c\mid d$,这就说明了,d 是最高公因子. ▎

引理 2 设 b 为正整数,a 为任意整数,则 a 和 b 的最高公式 d 可表为 $d=sa+tb$, $s,t\in\mathbf{I}$, $0\leqslant s<b$.

证明 若 $a=0$,则 b 就是 a,b 的最高公因子,$b=0a+1b$ 即为所求.

若 $a\neq 0$,利用上引理,必有 $j,h\in\mathbf{I}$ 使

$$d=ja+hb, \tag{*}$$

d 为 a,b 之最高公因子. 作除法,有

$$j = mb + s, \quad 0 \leqslant s < b,$$

代入($*$),得 $d = (mb+s)a + hb$,也就是

$$d = sa + (ma+h)b, \quad 0 \leqslant s < b. \qquad \blacksquare$$

推论 1 设 p 为素数. 对任意 $i^* \in \mathbf{I}_p$,如果 $i \neq 0$,则必有 $j < p$ 使 $i^* \times j^* = 1^*$.

事实上,i 和 p 的最高公因子为 1,据上引理,有 $j < p$ 使

$$1 = ji + mp, \quad 1^* = i^* \times j^*. \qquad \blacksquare$$

定义 2 设·为集合 A 上一运算. 若对任意 $a,b,c \in A$,都有

$$(a \cdot b) \cdot c = a \cdot (b \cdot c),$$

则说运算·满足**结合律**.

比如,例 1 中的 $\mathbf{I}$ 上乘法,例 2 中 $M_{n\times n}$ 上的加法,例 7 中子集的交运算和并运算,例 8 中向量的平行四边形合成运算,等等,都满足结合律.

例题 1 证明例 2 中 $M_{n\times n}$ 上运算,

$$A\theta B = A + B - AB,$$

也满足结合律.

证明 对任意 $A,B,C \in M_{n\times n}$,有

$$\begin{aligned}(A\theta B)\theta C &= (A+B-AB)\theta C = (A+B-AB)+C-(A+B-AB)C \\ &= A+B+C-AB-AC-BC+ABC,\end{aligned}$$

$$\begin{aligned}A\theta(B\theta C) &= A\theta(B+C-BC) \\ &= A+(B+C-BC)-A(B+C-BC) \\ &= A+B+C-BC-AB-AC+ABC,\end{aligned}$$

也就是 $(A\theta B)\theta C = A\theta(B\theta C)$, θ 满足结合律. $\blacksquare$

例题 2 证明例 9 中 $\mathbf{I}_n$ 上加法满足结合律.

证明 任取 $i^*, j^*, k^* \in \mathbf{I}_n$. 设

$$i + j = qn + r, \quad 0 \leqslant r < n, \tag{1}$$

$$j + k = pn + s, \quad 0 \leqslant s < n, \tag{2}$$

$$r+k=ln+t,\quad 0\leqslant t<n, \tag{3}$$
$$s+i=hn+u,\quad 0\leqslant u<n. \tag{4}$$
那么,应有
$$i^*+j^*=r^*,\quad j^*+k^*=s^*,$$
$$r^*+k^*=t^*,\quad s^*+i^*=u^*;$$
也就是
$$(i^*+j^*)+k^*=t^*,\quad i^*+(j^*+k^*)=u^*.$$
但是,把(3)代入(1),知
$$(i+j)+k=qn+r+k=(q+l)n+t,\quad 0\leqslant t<n, \tag{5}$$
而把(4)代入(2),得
$$i+(j+k)=i+s+pn=(k+p)n+u,\quad 0\leqslant t<n. \tag{6}$$
由除法余数的唯一性(实际上就是(6)减去(5)之两端,推出 $u-t$ 能被 n 整除,但 $-n<u-t<n$,必有 $u-t=0$, $u=t$)得到 $u=t$.所以,$t^*=u^*$, $\mathbf{I}_n$ 的加法满足结合律. ▌

仿此,可以证明 $\mathbf{I}_n$ 上的乘法也满足结合律.

例 5 中,$M(A)$上映射的复合运算也满足结合律,已在§4 命题 1 中证明.

例题 3 $\mathbf{I}$ 上减法(见例 4)不满足结合律.

证明 取整数 3,2,1∈$\mathbf{I}$,
$$(3-2)-1=0\neq 3-(2-1)=2,$$
即说明结合律不成立. ▌

例题 4 自然数 $\mathbf{N}$ 上运算 θ(见例 3),$m\theta n=m^n$,不满足结合律.

证明 取 2,1,3∈$\mathbf{N}$,则
$$(2\theta 1)\theta 3=2^1\theta 3=2^3=8,$$
$$2\theta(1\theta 3)=2\theta 1^3=2\theta 1=2^1=2,$$
即$(2\theta 1)\theta 3\neq 2\theta(1\theta 3)$. ▌

设·是集合 A 上的一个运算.如果它满足结合律,那么对任意三个元素 a,b,c(有顺序的)有$(a\cdot b)\cdot c=a\cdot(b\cdot c)$.而对于四元

有顺序的元素 $a,b,c,d\in A$，可计算出

$$((a\cdot b)\cdot c)\cdot d,\ (a\cdot b)\cdot(c\cdot d),\ a\cdot(b(c\cdot d))$$

及 $(a\cdot(b\cdot c))\cdot d$ 等 A 中元素，这些元素的关系如何呢？

一般来说，按顺序给定 A 的 n 个元素

$$a_1,a_2,\cdots,a_n$$

在指定的运算之下要对应 A 中一个元素，不单单与这些元素、与所给顺序有关，而且还与加括号程序（即运算程序）有关.

对于这给定的 n 个元素，只有有限种加括号的方法. 可分别记为

$$程序_i(a_1,\cdots,a_n),\quad i=1,2,\cdots,t.$$

特别地，记从前往后逐次加括号者

$$(\cdots(((a_1\cdot a_2)\cdot a_3)\cdot a_4)\cdots)\cdot a_n$$

为 $a_1\cdot a_2\cdot\cdots\cdot a_n$.

命题 1 给定 A 上运算·和任意（有序的）元素 $a_1,a_2,\cdots,a_n$，如果运算·满足结合律，那么 $i=1,2,\cdots,t$ 都有

$$程序_i(a_1,\cdots,a_n)=a_1\cdot a_2\cdot\cdots\cdot a_n.$$

证明 对 n 用数学归纳法.

当 $n=2,3$ 时，命题成立.

假设命题对于元素个数少于 n 个时成立. 我们研究 $a_1,\cdots,a_n$ 的一个运算程序

$$程序_i(a_1,a_2,\cdots,a_n).$$

不管中间加了多少括号，最后一步，必然是计算出来的两个元素运算. 不妨设为

$$程序_j(a_1,\cdots,a_m)\cdot程序_k(a_{m+1},\cdots,a_n),$$

其中 $0<m<n$. 程序$_j$ 是 m 个元素的一个运算程序，按归纳法假定，它等于

$$a_1\cdot a_2\cdot\cdots\cdot a_m.$$

程序$_k$ 是 $n-m$ 个元素的运算程序，$n-m<n$，按归纳法假定，它

等于

$$a_{m+1}\cdot\cdots\cdot a_n=(a_{m+1}\cdot\cdots\cdot a_{n-1})\cdot a_n.$$

所以,

$$\begin{aligned}程序_i(a_1,\cdots,a_n)&=(a_1\cdot\cdots\cdot a_m)\cdot(a_{m+1}\cdot\cdots\cdot a_n)\\&=(a_1\cdot\cdots\cdot a_m)\cdot((a_{m+1}\cdot\cdots\cdot a_{n-1})\cdot a_n).\end{aligned}$$

由 3 个元素的可结合性质知,它又等于

$$((a_1\cdot\cdots\cdot a_m)\cdot(a_{m+1}\cdot\cdots\cdot a_{n-1}))\cdot a_n.$$

再对前边 $n-1$ 个元素用归纳法假定,最后得

$$(a_1\cdot\cdots\cdot a_{n-1})\cdot a_n=a_1\cdot\cdots\cdot a_n. \qquad \blacksquare$$

今后,如果知道一运算满足结合律,可把 $a_1,\cdots,a_n$ 的任意一个(有序的)演算程序都写成 $a_1\cdot a_2\cdot\cdots\cdot a_n$.

定义 3 设·是集合 A 上的一个运算.如果,对任意 $a,b\in A$ 都有 $a\cdot b=b\cdot a$,则说运算·满足**交换律**.

比如 $\mathbf{I}$ 上加法和乘法,$\mathbf{I}_n$ 上加法和乘法,子集的交运算与并运算,等,都适合交换律.

而矩阵乘法,映射的复合运算,等等,都不适合交换律.

命题 2 设·是 A 上一个运算.如果运算·适合结合律和交换律,那么 n 个元素

$$a_1,a_2,\cdots,a_n$$

的任何一个顺序的任意一个运算程序

$$程序_l(a_{i_1},a_{i_2},\cdots,a_{i_n}),$$

都等于 $a_1\cdot a_2\cdot\cdots\cdot a_n$.其中 $i_1,i_2,\cdots,i_n$ 是数码 $1,\cdots,n$ 的一个排列.

证明 对 n 用数学归纳法.

当 $n=2$ 时,命题成立.

假定命题对元素个数少于 n 的情形成立.

对于

$$a=程序_l(a_{i_1},\cdots,a_{i_n}),$$

可设 $i_s = n$. 由命题 1 知

$$a = (a_{i_1} \cdot \cdots \cdot a_{i_{i-1}}) \cdot (a_{i_1} \cdot (a_{i_{i+1}} \cdot \cdots \cdot a_{i_n}))$$
$$= ((a_{i_1} \cdot \cdots \cdot a_{i_{i-1}}) \cdot (a_{i_{i+1}} \cdot \cdots \cdot a_{i_n})) \cdot a_n.$$

由归纳法假定上式之前括号中的元等于

$$a_1 \cdot a_2 \cdot \cdots \cdot a_{n-1},$$

从而 $a = (a_1 \cdot a_2 \cdot \cdots \cdot a_{n-1}) \cdot a_n$. ▌

历史上,人类最早学会的运算是正整数的加法. 经过多年实践,才认识到把“没有”记成数字 0 是非常方便的.

0 在整数集 **I** 的加法运算中有特殊作用,对任意 $m \in \mathbf{I}$,都有

$$m + 0 = m.$$

在其他的运算中,也常常见到这种元素,故有

定义 4 设·是集合 A 上的一个运算. 如果元素 $e \in A$ 对任何 $a \in A$ 都有

$$a \cdot e = e \cdot a = a,$$

则说 e 是 A 对于运算·的一个**单位元**或**恒等元**,也有人称之为**么元**、**中性元**.

例如,数 0 是整数集 **I** 对其上的加法运算的一个恒等元,因为对任意 $m \in \mathbf{I}$,都有 $m + 0 = 0 + m = m$.

数 1 是整数集 **I** 对其上的乘法运算的恒等元,因为对任意 $m \in \mathbf{I}$ 都有 $m \times 1 = 1 \times m = m$.

设 A 是集合,S 是 A 的所有子集的集合(例 7). 那么 A 是 S 上交集运算的恒等元,对任意 $U \subseteq A$,都有

$$U \cap A = A \cap U = U.$$

类似的,空集$\varnothing$是 S 上并集运算的恒等元,

$$U \cup \varnothing = \varnothing \cup U = U.$$

设 $M(A)$是非空集 A 上所有到 A 自身的映射的集合(例 5). 恒等映射 I_A 是 $M(A)$对映射复合运算的单位元.

0^* 是 $\mathbf{I}_n$ 对加法的恒等元,1^* 是 $\mathbf{I}_n$ 对乘法的恒等元.

例 2 中，规定

$$A\theta B = A + B - AB,$$

此运算之下零矩阵 $O_{n\times n}$ 为恒等元.

例 3 中，规定 $m\theta n = m^n$，在此运算之下 $\mathbf{N}$ 中无恒等元. 只要取数 2，若有 $t\in\mathbf{N}$，使

$$2\theta t = t\theta 2 = 2,$$

即 $2^t = t^2 = 2$，必导出矛盾.

偶数集在数的乘法运算之下，无恒等元.

命题 3 集合 A 对其上的运算 · 而言，如果有恒等元，则必唯一.

事实上，设 e, f 都是运算 · 之下的恒等元. 由于 e 是恒等元，故有

$$ef = fe = f;$$

而由 f 是恒等元，又应有

$$fe = ef = e;$$

所以 $e = f$. ▍

习 题 六

1. 在整数集 $\mathbf{I}$ 上，规定，任意 $m, n\in\mathbf{I}$ 对应

(a) $mn+1$; (b) m; (c) 2^{mn}; (d) 1

得到的 $\mathbf{I}$ 上运算中，哪些满足结合律，哪些满足交换律.

2. 完成下面的运算表，使其满足交换律

·	x	y	z	w
x	x	z		y
y		y		
z	w	x	y	
w		w	y	z

3. 证明：对任意 $r^*, s^*, t^*\in\mathbf{I}_n$，都有

$$(r^*+s^*)\times t^* = (r^*\times t^*)+(s^*\times t^*).$$

4. 设 θ 是集合 A 上的运算，τ 是集合 B 上的运算. 规定，任意

$(a_1,b_1),(a_2,b_2)\in A\times B$ 对应

$$(a_1\theta a_2,b_1\tau b_2),$$

则得 $A\times B$ 上一运算.进一步,如果 θ 和 τ 都满足结合律,则所得到的 $A\times B$ 上运算也满足结合律.

5. 设集合 A 仅由"好"、"坏"二字组成,A 上运算表是

⊙	好	坏
好	好	好
坏	好	坏

证明:该运算满足结合律和交换律,并找出恒等元.

6. 在整数集 I 上规定

$$m\odot n=2m+n^2,$$

则此运算不满足结合律,也不满足交换律,也没有恒等元.

小 结

本章内容是学习抽象代数必备的一些基础知识.

有些概念,如集合、子集、幂集、交集、并集、集合的笛卡尔积;映射、值域、定义域等在初等数学中就已出现过,相信读者接受起来无大问题.

抽象代数学主要讨论各种代数运算的运算规律.本章给出的运算概念是初等数学中"数的加法"、"多项式乘法"、"矩阵乘法"的推广.初学者每遇到一个新的"运算",应首先按定义检查一下它是否复合定义,然后进一步验证它是否满足结合律、交换律,有没有单位元.再就是将新的运算与你已知的数的运算、矩阵运算比较异同.温故而知新,你对已经见过的各种运算的性质认识得越深刻,那么你接受新的运算就会越快.

"映射"建立两个集合之间的联系.在今后讨论各种代数体系时都是最重要最基本的工具.同时,映射的合成给出了映射间的一种"运算";特别是置换的合成,将在本课程第二章与第三章中不断拿出来做例子.

所以，抽象代数学特别关注“合成”；关心一个映射是不是有逆，从而引出了“可逆映射”概念，也引出了“有左逆”和“有右逆”的讨论，这与映射是单的是满的有关系. §4 的定理 2 沟通了有逆与双射的关系.

关系、等价关系、分类与商集等内容是本章的重点，也是难点，是读者能否继续学习好本课程的关键之一. 复习总结时，可按例 11 讲解的顺序，通过这个实例搞清楚关系、反身性、对称性、传递性、等价类、分类、商集等概念的含义.

然后，再进一步从理论上弄通等价、分类、商集抽象定义的实质.

最后，如果你能自己举出实例来解释这些术语，才能真正地牢牢地记住它们.

书中提到的“完全集”概念已超出《考试大纲》的范围，当然不要求读者掌握. 但知道商集代表元选择中的种种问题有利于深刻理解商集的本性.

复 习 题

1. 设 A,B 是集合. 证明：$A\cup B=B$ 的充分必要条件是 $A\subseteq B$；$A\cap B=B$ 的充分必要条件是 $B\subseteq A$.

2. 设 A,B,C 是集合，且 $C\subseteq A$，$C\subseteq B$. 证明：

$$A\cap(B-C)=(A\cap B)-C.$$

3. 设 B 是个集合，且 $A_i\subseteq B$，$i\in\mathbf{I}$. 则必有

$$B-\bigcup_{i\in\mathbf{I}}A_i=\bigcap_{i\in\mathbf{I}}(B-A_i).$$

4. 用子集来描写映射关系. 在 $\mathbf{I}\times\mathbf{R}$ 中，下列哪些子集确定 $\mathbf{I}$ 到 $\mathbf{R}$ 的映射：

(a) $\{(m,m^2)\mid m\in\mathbf{I}\}$；

(b) $\{(2m,m)\mid m\in\mathbf{I}\}$；

(c) $\{(m,n)\mid |m|=|n|,\ m,n\in\mathbf{I}\}$；

(d) $\{(m,2m+1)\mid m\in\mathbf{I}\}\cup\{(m-1,2m-1)\mid m\in\mathbf{I}\}$.

5. 设 f 是 A 到 B 的映射，$f:A\rightarrow B$. 对任意 $x,y\in A$ 规定 xRy 当而且

只当$f(x)=f(y)$. 证明：R 是 A 上的等价关系.

设 $A=\{-2,-1,0,1,2,3\}$, $B=\{0,1,2,4,9\}$. 对任意 $x\in A$, $f(x)=x^2$. 求由这个 f 确定的关系 R，并用 $A\times A$ 的子集形式给出来.

6. 设 S 是所有平面三角形的集合. 设$\triangle ABC$，$\triangle A'B'C'$属于 S. 证明：平面几何学中$\triangle ABC \backsimeq \triangle A'B'C'$（相似），是个等价关系.

7. 设 f 是复数集 $\mathbf{C}$ 到 $\mathbf{C}$ 的映射，

$$f(x)=x^2,\quad x\in\mathbf{C},$$

而 g 是实数集 $\mathbf{R}$ 到 $\mathbf{R}$ 的映射 $g(y)=y^2$, $y\in\mathbf{R}$. 设

$$S_1=\{m^2\mid m\in\mathbf{I}\},\quad S_2=\{1,-1\},\quad S_3=\{m\mid m\in\mathbf{I}\},$$

分别求出 $f^{-1}(S_1),g^{-1}(S_1),f^{-1}(S_2),g^{-1}(S_2),f^{-1}(S_3),g^{-1}(S_3)$.

8. 设 f 是正整数集 $\mathbf{N}$ 到 $\mathbf{N}$ 的映射，

$$f: i\to i+1,\quad i\in\mathbf{N}.$$

证明：可以找到无穷多个 $\mathbf{N}$ 到 $\mathbf{N}$ 的映射 g 使得$g\cdot f$ 等于 $\mathbf{N}$ 上的恒等映射，但 $\mathbf{N}$ 到 $\mathbf{N}$ 的任何映射 h 均不能使得$f\cdot h$ 为恒等映射.

9. 设·是集合 S 上的一个二元运算，满足结合律. 那么对于 S 的幂集 2^S（所有 S 的子集的集合）规定，对任意 $A,B\in 2^S$，也就是 $A,B\subseteq S$，对应 2^S 的元素（S 的子集）

$$\{a\cdot b\mid a\in A,\ b\in B\},$$

并把这个子集记为 $A\odot B$. 证明：$\odot$是 2^S 上的结合的二元运算.

10. 在 $\mathbf{I}$ 上规定对任意 $m,n\in\mathbf{I}$,

$$m*n=m+n-mn,$$

其中右端的加、减、乘均为通常的数的运算. 证明：$*$ 是 $\mathbf{I}$ 上结合的、交换的运算，而且有恒等元.

第二章 群与子群

一个集合,对于它上的一个运算,满足结合律等几条极简单而又极自然的要求,即说该集合对这个运算构成群.

物理学、化学、生物学,甚至社会科学中都有很多很有趣的群的例子.群的研究工作是有广泛的实际背景的.

群又是抽象代数学中最基本的代数体系,是本课程要讨论的其它各种代数体系的基础.

一般来说,学习群的理论要从两个方面入手.

一是先搞懂定义,群是什么东西,它包含哪些对象,有哪些基本性质,它有哪些分类的办法.

另一个方面是,怎样的两个群,从代数学的观点来看是一样的,只要研究了一个,另一个就完全清楚了.怎样的两个群,从代数学观点来看,一个是另一个的"缩影".怎样的群可以看成是由更简单的群"拼凑"而成的.

后者是我们要在第三章讨论的主要内容,前者就是本章要处理的问题

§1 群的定义

定义 1 一个集合 G 和 G 上的一个运算·满足下列条件,则说 G 对·构成群,或说 $(G,\cdot)$ 是个群,在不致引起混乱时(即从上下文可以清楚判断所说的运算时)也可以简单地说,G 是个群:

(1) 结合律;

(2) 有**恒等元**,即有 $e\in G$,对任意 $a\in G$,都有

$$e\cdot a=a\cdot e=a;$$

(3) 每个元都有**逆元素**,即对任意 $a\in G$,都有 $b\in G$ 使得

$$a\cdot b=b\cdot a=e.$$

例 1 (I, +)是个群.

我们已经知道,(I, +)满足结合律,0 是恒等元. 进一步,对任意整数 m,整数 $-m$ 使得

$$m+(-m)=(-m)+m=0.$$

例 2 (I, ×)不是群. 虽然,它满足结合律,有恒等元 1,有些元素有逆元,如对 1 有元素 1 使 1×1=1×1=1,对 -1 有元素 -1 使

$$(-1)\times(-1)=(-1)\times(-1)=1,$$

但不存有整数 n 使 $2\times n=1$.

只要有一个元素没有逆元,即可说明这不构成群.

例 3 设 N 为正整数作成的集合. 它对于数的加法 + 不构成群,因为它没有恒等元. 如果把 N 添上 0 作成非负整数的集合 M,那么(M, +)也不是群,因为 1 无逆元.

例 4 集合{0}在数的加法之下,构成群.

例 5 所有正的有理数的集合 A,在数的乘法之下作成群.

首先要验证:数的乘法确实是 A 上的一个运算. 设 $m/n, p/q\in A$,则整数 m,n 同号,整数 p,q 同号,所以 mp, nq 同号,即

$$mp/(nq)\in A.$$

其次,A 对数的乘法当然满足结合律.

再次,1 是 A 在乘法之下的恒等元.

最后,对任意 $m/n\in A$,由于 m,n 是同号的非零整数,知 $n/m\in A$,且

$$(m/n)\times(n/m)=1.$$

即 A 的每个元素都有逆.

所以,(A, ×)构成群.

例6 第一章§6之例5，A为非空集合，$I(A)$为所有A到A的双射的集合，$\circ$为映射的复合运算，则$(I(A),\circ)$是个群. 因为，在前一章，我们已经证明了，两个双射的复合确为双射，映射的复合满足结合律，恒等映射i_A使得对任意$f\in M(A)$都有$f\circ i_A=i_A\circ f=f$. 还证明了，每个双射f都有逆映射g使之

$$f\circ g=g\circ f=i_A.$$

但是，当A的元素的个数大于1时，A到A的所有映射的集合$M(A)$，在映射的复合之下不构成群.

取$a\in A$，规定A中每个元都对应a，所得之映射f不是满射. 由第一章§4定理2知f不是可逆映射，也就是f没有逆元素.

读者先复习一下第一章§6的例9，然后看下面的两个例子.

例7 对任意正整数n，$(\mathbf{I}_n,+)$是个群.

例8 对任意素数p，令A为$\mathbf{I}_p$中去掉元素0^*后所余元素的集合，即

$$A=\{1^*,2^*,\cdots,(p-1)^*\}.$$

按$\mathbf{I}_p$的乘法规定A的乘法$\times$，则$(A,\times)$为一个群.

首先，要说明$\mathbf{I}_p$的乘法确实可在A上导出一个运算. 也就是要说明，按$\mathbf{I}_p$的乘法，A的任意元素r^*，s^*对应的$r^*\times s^*$确实是A中元素. 而A与$\mathbf{I}_p$差别只在元素0^*，也就是说，要证明$r^*\neq 0^*$，$s^*\neq 0^*$时$r^*\times s^*\neq 0^*$.

事实上，r和s不为0且小于p，它们与p互素，故$p\nmid(rs)$，rs用p除不会余0，故$r^*\times s^*\neq 0^*$.

其次，要说明A对此乘法满足结合律.

再次，可以看出1^*是A在该运算之下的恒等元. 以上两款都是很自然的事情.

最后，要说明，当$r^*\neq 0^*$时，即$r^*\in A$则必有$t^*\in A$使$r^*\times t^*=t^*\times r^*=1^*$. 这个问题，我们已在前一章§6引理的推

论中解决过了.

例 9 对任意给定的实数对(a,b), $a\neq 0$,用 $f_{a,b}$代表 **R** 到 **R** 的映射,对任意 $x\in\mathbf{R}$, $f_{a,b}=ax+b$.令

$$A=\{f\in M(\mathbf{R})\mid f=f_{a,b},\ a,b\in\mathbf{R},\ a\neq 0\}.$$

对任意 $f_{a,b},f_{c,d}\in A$,由于

$$(f_{a,b}\circ f_{c,d})(x)=f_{a,b}(f_{c,d}(x))=f_{a,b}(cx+d)$$
$$=acx+ad+b,$$

且 $ac\neq 0$,故

$$f_{a,b}\circ f_{c,d}=f_{ac,ad+b}\in A.$$

这说明,映射的复合是 A 上的一个运算.当然满足结合律.

由于 $f_{1,0}(x)=1\cdot x=i_{\mathbf{R}}(x)$, $f_{1,0}$即为 A 的恒等元.

对任意 $f_{a,b}\in A$,由于 $a\neq 0$,故 a 的倒数 $a^{-1}\neq 0$.从而 $f_{a^{-1},-a^{-1}b}\in A$,且

$$f_{a,b}\circ f_{a^{-1},-a^{-1}b}=f_{a^{-1},-a^{-1}b}\circ f_{a,b}=i_{\mathbf{R}}.$$

也就是 $f_{a,b}$有逆.

所以,$(A,\circ)$是个群.

下面,我们看,一个群具有怎样的简单性质.将来,一旦验证了某个集合及其上的一个运算满足了群的定义中的三条要求,那么,它就一定有这些性质,就不需每次都来证明它有这种共性了.这正是公理化方法的优点.

命题 1 设$(G,\cdot)$是个群,那么 G 中任意元素 a 只有唯一的一个逆元素.

证明 设有 $x,y\in G$ 使得

$$x\cdot a=a\cdot x=e,\quad y\cdot a=a\cdot y=e,$$

其中 e 为 G 之单位元.于是

$$\begin{aligned} x&=x\cdot e && (e\text{ 为单位元})\\ &=x\cdot(a\cdot y) && (a\cdot y=e)\\ &=(x\cdot a)\cdot y && (\text{结合律}) \end{aligned}$$

$$= e \cdot y \qquad (x \cdot a = e)$$
$$= y. \qquad (e \text{ 为单位元})$$ ▌

既然群 G 的每个元素 a 都唯一确定一个逆元,我们就将 a 的逆记为 a^{-1}. 即

$$a \cdot a^{-1} = a^{-1} \cdot a = e,$$

其中 e 经常用来代表群的单位元. 当涉及到的群比较多时,再用 e_G 表示是 G 的单位元,有时还要详细指出是对何种运算而言的单位元.

进一步,当集中精力只讨论一种运算,常将运算符号省掉,简记 $(G,\cdot)$ 为 G,且记 $a \cdot b = ab$.

命题 2 设 G 是个群. 对任意 $a, b \in G$ 有

$$(a^{-1})^{-1} = a, \quad b^{-1}a^{-1} = (ab)^{-1}.$$

证明 由于 a^{-1} 是 a 的逆,故有

$$aa^{-1} = a^{-1}a = e.$$

这也说明,对于元素 a^{-1},我们有元素 a 使得它们满足上式. 据定义 a 是 a^{-1} 的一个逆,逆元素是唯一确定的,a^{-1} 的逆元应记为 $(a^{-1})^{-1}$. 故

$$a = (a^{-1})^{-1}.$$

又由

$$(b^{-1}a^{-1})(ab)$$
$$= b^{-1}(a^{-1}a)b \qquad (\text{结合律})$$
$$= b^{-1}(eb) \qquad (a^{-1}a = e, \text{结合律})$$
$$= b^{-1}b \qquad (e \text{ 为单位元})$$
$$= e, \qquad (b^{-1} \text{是 } b \text{ 的逆元})$$

以及 $(ab)(b^{-1}a^{-1}) = e$,即知 $b^{-1}a^{-1}$ 是 ab 的逆元素,从而

$$(ab)^{-1} = b^{-1}a^{-1}.$$ ▌

命题 3 设 G 为群. 对任意 $a, b, c \in G$, $ab = ac$ 蕴涵 $b = c$, $ba = ca$ 蕴涵 $b = c$,并分别称为左、右消去律.

证明 若 $ab = ac$,用元素 a^{-1} 乘等式两端,有

$$
\begin{aligned}
a^{-1}(ab) &= a^{-1}(ac), \\
(a^{-1}a)b &= (a^{-1}a)c, && \text{(结合律)} \\
eb &= ec, && (a \text{ 和 } a^{-1} \text{互为逆元}) \\
b &= c. && (e \text{ 是单位元})
\end{aligned}
$$

同理可证群满足右消去律. ▎

推论 1 如果 G 是个群,$a_1,\cdots,a_k\in G$,则

$$(a_1a_2\cdots a_k)^{-1}=a_k^{-1}\cdots a_1^{-1}.$$

读者可用数学归纳法自证之. ▎

定理 1 设·是集合 G 上的一个运算,只要它们满足

(1) 结合律,

(2) 有**左单位元** e,即有 $e\in G$,对任意 $a\in G$ 都有 $ea=a$,

(3) 有**左逆元**,对于 e,每个元素 $a\in G$ 都有 $b\in G$ 使得 $ba=e$,

则$(G,\cdot)$是个群.

证明 这组条件与群的定义中要求的条件相比,可以看出,我们只要证明这个元素 e 对任何 $a\in G$ 能够有 $ae=a$,同时 $ba=e$ 蕴涵 $ab=e$ 就行了.

对任意 $a\in G$,有 $b\in G$ 使得 $ba=e$. 但对于得到的 b,也应该有 c 使 $cb=e$,这样

$$
\begin{aligned}
ab &= e(ab) && (e \text{ 是左单位元}) \\
&= cb(ab) && (cb=e) \\
&= c(ba)b && \text{(结合律)} \\
&= cb && (ba=e,\ e \text{ 为左单位元}) \\
&= e. && (cb=e).
\end{aligned}
$$

进而,还有

$$
\begin{aligned}
ae &= a(ba) && (ba=e) \\
&= (ab)a && \text{(结合律)} \\
&= ea && (ab=e,\text{刚刚证得}) \\
&= a. && (e \text{ 是左单位元})
\end{aligned}
$$
▎

这样,在验证集合 G 和它上的一个运算·构成群时,可以用表

而上比较弱的条件来代替形式上要求较强的条件(实际上,我们已经证明了,它们是等价的).

定理 2 设$\cdot$是集合 G 上的一个运算且满足结合律.那么,$(G,\cdot)$是个群,必要而只要,对任意 $a,b\in G$ 都有唯一确定的$c,d\in G$ 使得$a\cdot c=b$, $d\cdot a=b$.

证明 如果$(G,\cdot)$是个群,那么对任意 $a,b\in G$,取 $c=a^{-1}\cdot b$, $d=b\cdot a^{-1}$,则

$$a\cdot c=b,\quad d\cdot a=b. \tag{2}$$

由于群满足消去律,使(2)成立的 c 和 d 都是唯一确定的.

反过来,如果对任意的 $a,b\in G$,都有唯一确定的 c,d 使(2)成立.那么,由于 G 不是空集,我们可任取一 $g\in G$,据条件,对 g,g 应有 e 使得$e\cdot g=g$.可证明,这样得到的元素 e 实际上是个左单位元.

对任意 $a\in G$,据条件,相应于 a,g 又必$h\in G$ 使得$g\cdot h=a$,于是

$$\begin{aligned}
e\cdot a&=e\cdot(g\cdot h) && (g\cdot h=a)\\
&=(e\cdot g)\cdot h && (\text{结合律})\\
&=g\cdot h && (e\text{ 对 }g\text{ 有特殊作用},e\cdot g=g)\\
&=a. && (g\cdot h=a)
\end{aligned}$$

再来证明,对于 e,每个 $a\in G$ 都有左逆元.据条件,对 a,e 应有 d 使得$d\cdot a=e$.

据定理 1, $(G,\cdot)$为群. ▌

由于群的运算满足结合律,群的一个元素 a,按任何加括号程序运算 n 次,其结果总是一样的,可记为 $aa\cdots a$(n 个a),简记为a^n.再规定元素 a 的负整数次方为

$$a^{-n}=(a^n)^{-1},$$

以及 $a^0=e$.

命题 4 对任意正整数 n,都有 $a^{-n}=(a^{-1})^n$.

证明 给定了群的一个元素 a 和一个正整数n, a^n,a^{-1}都是

该群的确定的元素. $(a^{-1})^n$ 也是这个群的一个确定的元素，要证明它是元素 a^n 的逆元素，可对 n 用数学归纳法.

当 $n>1$ 时，

$$\begin{aligned} & a^n(a^{-1})^n \\ & = a^{n-1}(aa^{-1})(a^{-1})^{n-1} \quad (a^n \text{ 的定义，结合律}) \\ & = a^{n-1}(a^{-1})^{n-1} \quad (a^{-1}\text{是 } a \text{ 的逆}) \\ & = e. \quad (\text{归纳法假定}) \end{aligned}$$

从定理 2 的证明中可以看出，在群中，一个元素是另一元素的左逆元就必然是该元素的逆元·故 $(a^{-1})^n$ 为 a^n 的逆元. ∎

命题 5 设 a 是群 G 的一个元素. 对任意整数 m,n 都必有

$$a^na^m = a^{m+n}, \quad (a^n)^m = a^{mn}.$$

证明 若 $m=0$，那么，$a^0=e$，

$$a^na^0 = a^n = a^{n+0}, \quad (a^n)^m = e = a^{mn}.$$

当 $n=0$ 时，命题可同理证明之.

当 m,n 都是正整数时，a^na^m 乃是 n 个 a 与 m 个 a 相乘，其结果是 $m+n$ 个 a 相乘，即

$$a^na^m = a^{m+n}.$$

而 $(a^n)^m$ 乃是 m 个 a^n 的乘积，a^n 又是 n 个 a 相乘，其结果恰为 mn 个 a 的乘积，即

$$(a^n)^m = a^{mn}.$$

当 m 是正整数，$n=-l$ 是负整数时，$a^n = a^{-l} = (a^{-1})^l$. 从而 a^na^m 乃是 l 个 a^{-1} 和 m 个 a 的乘积. 其结果，当 $m-l=m+n>0$ 时，为 $m+n$ 个 a 的乘积，即

$$a^na^m = a^{m-l} = a^{m+n};$$

当 $m=l$ 时，a 的个数与 a^{-1} 个数相同，即

$$a^na^m = e = a^{m+n};$$

当 $m-l<0$，为 $l-m$ 个 a^{-1} 之积，即

$$a^na^m = (a^{-1})^la^m = (a^{-1})^{l-m} = a^{m-l} = a^{m+n}.$$

也就是说，m 为正整数，n 为负整数时，恒有 $a^na^m = a^{m+n}$.

对于 m 为负，n 为正数的情形，证明步骤相同. 只要记住，元素 a 的 $-n$ 方，$n>0$，即是 a^n 的逆元又是 n 个 a^{-1} 的乘积即可.

对于 m,n 均为负整数情形，$a^m a^n$ 和 a^{m+n} 乃是同样多个 a^{-1} 的乘积.

关于命题的第二个等式，也可分别 m,n 正负情形讨论. 例如，当 m 为正，$n=-l$ 为负时，

$$(a^n)^m=(a^{-l})^m=[(a^{-1})^l]^m=a^{-lm}=a^{nm}.$$

余者仿此可证. ▌

群 $(G,\cdot)$ 的运算通常称为乘法. 当群的运算 $\cdot$ 满足交换律时，则称之为**交换群**或**阿贝尔（Abel）群**. 交换群的运算可称为**加法**.

交换群 G 的单位元称为**零元素**，记为 0. 运算符号用 $+$. 于是，对任意 $a\in G$，有 $a+0=0+a=a$.

同时，在交换群中，元素 a 的逆元素改称为 a 的**负元素**，并记为 $-a$. 把 m 个 a 相加记为 ma.

对于正整数 n，记

$$(-n)a=-(na),\quad 0\cdot a=0.$$

则命题 5 对交换群 $(G,+)$ 而言，就成为

$$na+ma=(m+n)a,\quad n(ma)=(nm)a,$$

对任意整数 m,n 和任意 $a\in G$ 都成立.

为了熟悉群的运算特点，让我们研究几个例题.

例题 1 验证所有形如

$$2^m 3^n,\quad m,n \text{ 是整数},$$

的有理数的集合 G，在数的乘法之下构成群.

证明 首先，对 G 中任意两个有理数

$$2^m 3^n,\quad 2^p 3^q,$$

由于 m,n,p,q 都是整数，故 $m+p,n+q$ 也是整数，从而

$$2^m 3^n\times 2^p 3^q=2^{m+p}3^{n+q}\in G;$$

也就是说，数的乘法确实是 G 上的运算.

这种运算满足结合律和交换律.

其次，取 $m=n=0$ 得 G 中有理数

$$2^0 3^0=1,$$

它与 G 之每个数 $2^p 3^q$ 相乘仍得 $2^p 3^q$，即 1 是 G 之恒等元.

最后，任取 $2^m 3^n \in G$，m,n 是整数. 于是 $-m$，$-n$ 也是整数，故 $2^{-m}3^{-n}\in G$. 同时还有 $2^m 3^n \times 2^{-m} 3^{-n}=1$，即 G 的每个元素都在 G 中有逆元.

所以，$(G,\times)$是个群. ▌

虽然数乘是满足交换律的，由于人们对这种运算的记号太熟悉了，通常就不把它改称为"加"了.

例题 2 在群 G 中，令 e 是它的恒等元. 那么，对任意 $x,y\in G$，只要 $xy=e$，则必然有 $yx=e$.

证明 将 $xy=e$ 之两端同乘 x 的逆元 x^{-1}，得

$$x^{-1}(xy)=x^{-1}e,\quad (x^{-1}x)y=x^{-1},\quad y=x^{-1},$$

这说明 y 从两侧乘 x 都得 e. ▌

此事实我们在命题 4 的证明中已经使用过了.

例题 3 在群 G 中，若 $x,y\in G$，则称元素 $xyx^{-1}y^{-1}$ 为 x,y 的**换位子**，记为

$$[x,y]=xyx^{-1}y^{-1}.$$

证明：对任意 $x,y\in G$，恒有$[x,y]^{-1}=[y,x]$.

证明 这个等式就是要证明$[y,x]$是元素$[x,y]$的逆元，即

$$[x,y][y,x]=1,\quad [y,x][x,y]=1.$$

而由例题 2 又知，只要证明上述两等式中的一个就足够了.

事实上，

$$\begin{aligned}
&[x,y][y,x]\\
&=(xyx^{-1}y^{-1})(yxy^{-1}x^{-1}) &&(\text{定义})\\
&=(xyx^{-1})(y^{-1}y)(xy^{-1}x^{-1}) &&(\text{结合律})\\
&=xy(x^{-1}x)y^{-1}x^{-1} &&(\text{逆元性质})\\
&=1. &&(\text{逆元性质})
\end{aligned}$$

▌

例题 4 已知 x,y 是群 G 的元素，且

$$x^2y=y^2x,\quad x^8=1.$$

证明：$(xy)^4=1$，$y^8=1$.

证明 由 $x^2y=y^2x$ 得到 $x^2=y^2xy^{-1}$，故

$x^8=(x^2)^4=(y^2xy^{-1})(y^2xy^{-1})(y^2xy^{-1})(y^2xy^{-1})=1$,

$x^8=(y^2x)yxyxyxy^{-1}=1$.

用例题 2，得

$$(xyxyxyxy^{-1})y^2=1,$$

也就是 $(xy)^4=1$.

又因为 $y^2=x^2yx^{-1}$，故

$y^8=(y^2)^4=(x^2yx^{-1})^4=x^2yxyxyxyx^{-1}$,

$y^8=x(xy)^4x^{-1}=xx^{-1}=1$. ▌

习 题 一

1. 设 f,g 是 $(0,+\infty)$ 到 $(0,+\infty)$ 的映射（也就是实函数），对任意 $x\in(0,+\infty)$ 有

$$f(x)=x,\quad g(x)=1/x.$$

证明：集合 $\{f,g\}$ 在映射合成之下是个群.

2. 在整数集 $\mathbf{I}$ 上，规定运算·，对任意 $a,b\in\mathbf{I}$,

$$a\cdot b=a+b-2.$$

证明：$(\mathbf{I},\cdot)$ 是个群.

3. 设 G 是个群，$a\in G$. 证明：$aa=a$，必要而只要 a 为 G 的单位元.

4. 设 F 是定义在 $(-\infty,\infty)$ 上的所有实函数的集合，规定，对任意 $f,g\in F$，$f\# g: x\mapsto f(x)+g(x)$，$x\in\mathbf{R}$，证明：$(F,\#)$ 是个加法群.

5. 设 $(G,*)$ 是个群，完成下面的乘法表

*	a	b	c
a		b	
b			
c			

并说明此表填法是唯一确定的.

6. 设 G 是个群.证明:G 为交换群的充分必要条件是对任意$a,b\in G$,

$$(ab)^{-1}=a^{-1}b^{-1}.$$

7. 在集合 $\mathbf{R}-\{1\}$上定义乘法

$$x\# y=x+y-xy,\quad x,y\in\mathbf{R},\ x\neq 1,\ y\neq 1.$$

证明:$(\mathbf{R}-\{1\},\#)$是个交换群.

§2 子　　群

偶数集是整数集的子集,在整数的加法之下,偶数集本身构成群.

几何空间中,向量在平行四边形法则规定的向量加法之下构成群.而该空间中,对任意取定的平面,这个平面上的所有向量在向量加法之下也构成一个群.

那么,当已经知道整数加群、几何空间向量加群有某些性质,是否能轻而易举地知道偶数加法群、平面向量加法群也有相应性质呢?

因为,今后要反复地提到集合和它的子集合对相应运算构成的群,我们给出

定义 1 设$(G,\cdot)$是个群,如果 G 的子集 H 对于$\cdot$也构成群,则说$(H,\cdot)$是$(G,\cdot)$的子群.或者,简单地说,H 是 G 的子群.

例 1 在整数加法群$(\mathbf{I},+)$中,偶数集在加法之下为$(\mathbf{I},+)$的子群;$\{\cdots,-n,0,n,\cdots\}$也是$(\mathbf{I},+)$的子群;$\{0\}$是子群;$(\mathbf{I},+)$本身是自己的子群.非负整数集不是$(\mathbf{I},+)$的子群.

例 2 $(\mathbf{I}_6,+)$中,$\{0^*,2^*,4^*\}$,$\{0^*,3^*\}$分别是子群.

由定义立刻可以看出,若群$(G,\cdot)$的子集 H 是子群,群 G 上的运算$\cdot$必须是 H 上的运算;也就是说 $G\times G$ 到 G 的这个对应规则必须是 $H\times H$ 到 H 的对应规则;换句话说,对任意 $a,b\in H$,必须有

$$a\cdot b\in H.$$

H 对·满足结合律是自动成立的.因为对任意 $a,b,c\in G$，在 G 里已知

$$(a\cdot b)\cdot c=a\cdot(b\cdot c),$$

那么 $H\subseteq G$，H 中元素运算当然满足结合律了.

命题 1 如果 H 是 G 的子群，那么 H 的恒等元 f 等于 G 的恒等元 e；也就是说 $e\in H$.

证明 由 f 是 H 的恒等元知 $ff=f$. 作为 G 中的元素，f 在 G 中有逆元素 f^{-1}，于是

$$ff=f,$$

$$fff^{-1}=ff^{-1},\qquad\text{（两端右乘 }f^{-1}\text{）}$$

$$f=e.\qquad\text{（}f^{-1}\text{是 }f\text{ 在 }G\text{ 中的逆）}\qquad\blacksquare$$

下面定理能帮助我们用更简便的方法来验证群 G 的子集 H 是否是 G 的子群.

这些证明的关键是要牢牢掌握住，H 的运算就是 G 中原来的运算，不是另搞一套.例如，不能说，非零实数的集合在数的乘法之下构成的群是实数加法群的子群.

定理 1 设 $(G,\cdot)$ 是个群，H 是 G 的子集.那么，H 是 G 的子群，当而且仅当

(1) H 非空，

(2) 如果 $a,b\in H$，则 $a\cdot b\in H$，

(3) 如果 $a\in H$，则 a 在 G 中的逆元 $a^{-1}\in G$.

证明 设 H 是 G 的子群.那么，作为一个群，H 上有运算·，它是非空的. H 满足(1).

要使·成为 H 上的运算，上面已经分析过了，它必然满足条件(2)，即对任意 $a,b\in H$，有 $a,b\in H$.

现在来验证条件(3). H 在·之下作成群，据命题 1，G 的恒等元 e 就是 H 的恒等元. $a\in H$，作为群 H 的元素，在 H 中应有逆元 b，也就是有 $b\in H$ 使 $b\cdot a=a\cdot b=e$. 但是，a 作为群的元素在 G

中应有逆元a^{-1}，于是

$$\begin{aligned} a^{-1} &= e\cdot a^{-1} && (e\text{ 是 }G\text{ 的恒等元}) \\ &= (b\cdot a)\cdot a^{-1} && (e\text{ 又是 }H\text{ 的恒等元}) \\ &= b\cdot(a\cdot a^{-1}) && (\text{结合律}) \\ &= b\cdot e && (a^{-1}\text{是 }a\text{ 的逆元素}) \\ &= b. \end{aligned}$$

由于 $b\in H$，证明了 $a^{-1}\in H$.

反过来，设 H 是 G 的子集，且满足条件(1)，(2)和(3).

这时，(1)和(2)保证了·是集合 H 上的一个运算，H 中任意两个元素 x,y 在 G 的运算·之下确定对应 H 中一个确定元素.

H 是 G 的子集，在同一运算之下，G 的元素满足结合律，当然，H 的元素亦满足结合律.

先断言 H 必含 G 之恒等元 e. H 非空，必有 $a\in H$. 由条件(3)知，a 在 G 中的逆元素 a^{-1} 亦在 H 中. 再据条件(1)，得到 $a\cdot a^{-1}=e\in H$. e 在 H 中，对任意 $x\in H$ 都有 $e\cdot x=x\cdot e=x$，从而 e 必为 H 的恒等元.

最后，可证明对任意 $x\in H$，x 在 H 中有逆元 y 使得

$$x\cdot y=y\cdot x=e. \tag{3}$$

这是因为 H 的恒等元 e 就是 G 的恒等元，而由条件(3)知 x 在 G 中的逆 $x^{-1}\in H$. 把这个元素 x^{-1} 放到 y 的位置上，即知式(3)成立.

这说明 H 在·之下构成群. ▌

定理 2 设 G 是个群，H 是 G 的子集. 那么，H 是 G 的子群，当而且仅当

(1)* H 非空，

(2)* 对任意 $a,b\in H$，都有 $ab^{-1}\in H$.

证明 就是要证这里的(1)*，(2)*与定理 1 中的(1)，(2)和(3)等价. 其中(1)*和(1)是一样的.

若 H 满足(2)和(3). 对任意 $a,b\in H$，由(3)推出 $b^{-1}\in H$，再

据(2)，$a, b^{-1} \in H$，应有 $a \cdot b^{-1} \in H$. 也就是 H 满足(2)*.

若 H 满足条件(2)*、任取 H 中一个元素 a，由 $a, a \in H$ 得 $aa^{-1} = e \in H$. 再由 $e, a \in H$ 得

$$ea^{-1} = a^{-1} \in H.$$

说明条件(3)成立.

进而，对任意 $a, b \in H$，已证得有 $b^{-1} \in H$，由 $a, b^{-1} \in H$，套用条件(2)*，得

$$a \cdot (b^{-1})^{-1} = ab \in H.$$

也就是 H 满足(2). ▌

例题 1 G 是所有 n 阶非奇异实矩阵在矩阵乘法之下作成的群. 证明：所有行列式值等于 1 的 $n \times n$ 实矩阵的集合 H 是 G 的一个子群.

证明 单位矩阵之行列式为 1，故 H 非空.

设 $A, B \in H$，则 $|A| = |B| = 1$，从而

$$|AB| = |A||B| = 1,$$

即 $AB \in H$.

对任意 $A \in H$，$|A| = 1$，则 A 的逆矩阵 A^{-1} 的行列式值亦为 1，即

$$A^{-1} \in H.$$

这就验证了 H 是 G 的子群. ▌

命题 2 设 G 是个群. 对于 G 的任意一个子群族

$$\{H_j \subseteq G \mid H_j \text{ 为 } G \text{ 的子群}, j \in J\}$$

其交集 $H = \bigcap_{j \in J} H_j$ 仍为 G 的子群.

证明 G 的恒等元 e 在每个子群 H_j 中，从而亦在它们的交集之中，即 $\bigcap_{j \in J} H_j$ 非空.

对任意 $a, b \in H$，由于 H 是交集，故对任意 $j \in J$，都有 $a, b \in H_j$. 而 H_j 是 G 的子群，由定理 1 知 $ab \in H_j$ 对任意 $j \in J$ 都成立，据此，得到 $ab \in H$.

对任意 $a\in H$，则 $a\in H_j$，$j\in J$. 而 H_j 为 G 的子群，再次用定理 1，推出，对每个 $j\in J$ 都有 $a^{-1}\in H_j$，据此，得 $a^{-1}\in H$.

这就证明了 H 是 G 的子群. ∎

对于子群的并集，不能照搬交集的结果. 例子读者可自己给出.

例题 2 设 H 和 K 都是群 G 的子群. 如果并集 $H\cup K$ 也是 G 的子群，那么必有 $H\subseteq K$ 或者 $K\subseteq H$.

证明 用反证法. 设 $H\cup K$ 是 G 的子群，且有 $k\in K$，$k\notin H$，有

$$h\in H,\quad h\notin K.$$

由于 $k\in K$，$h\in H$，故 $k,h\in K\cup H$. 但 $K\cup H$ 是 G 的子群，从而 k 和 h 的乘积 $kh\in K\cup H$（定理 1）.

kh 在 K 和 H 的并集中，则只少在它们里的一个之中. 若 $kh\in K$. 由 $k\in K$，$k^{-1}\in K$ 即得

$$k^{-1}(kh)=(k^{-1}k)h=h\in K,$$

矛盾. 若 $kh\in H$，同理可知，$k\in H$，亦为矛盾. ∎

例题 3 设 G 是个群. 集合

$$C=\{a\in G\mid ax=xa,\text{对所有 } x\in G\}$$

是 G 的一个子群，此群称为群 G 的**中心**.

证明 首先，G 的恒等元 e 与 G 之任意元 x 可交换，$xe=ex=x$，故 $e\in C$，C 非空.

其次，对任意 $a,b\in C$，任取 $x\in G$，有

$$\begin{aligned}(ab)x&=a(bx) &&\text{（结合律）}\\ &=a(xb) &&(b\in C,\ b,x\text{ 可交换})\\ &=x(ab). &&(a\in C)\end{aligned}$$

即知 $ab\in C$.

最后，若 $a\in C$，那么，对任意 $x\in G$ 有

$$xa=ax.$$

将等式左乘 a^{-1}，再右乘 a^{-1}，得

$$(a^{-1}x)(aa^{-1})=(a^{-1}a)(xa^{-1}),\quad a^{-1}x=xa^{-1},$$

即 $a^{-1}\in C$.

所以,据定理 1, C 为 G 的子群. ▌

现在,设 S 是群 G 的一个非空子集,我们来看 G 的子群族

$$\mathscr{F}=\{H\subseteq G\mid S\subseteq H,\ H\text{ 为 }G\text{ 的子群}\}.$$

由于 $S\subseteq G$, $G\in\mathscr{F}$, $\mathscr{F}$ 非空,故 $\mathscr{F}$ 中所有子群的交集仍为 G 之子群.

定义 2 设 G 是个群, S 为其一非空子集合. $\mathscr{F}$ 为 G 的所有包含 S 的子群的族,则称子群

$$\bigcap_{H\in\mathscr{F}}H$$

为 S 在 G 中**生成的子群**,记为 $\langle S\rangle$.

我们先来考查群 G 中一个元素 a 构成的子集 $S=\{a\}$ 的情形. 看 a 的所有整数次方所构成的 G 的子集 $\{a^i\mid i\in\mathbf{I}\}$,当然,可能有 $i,j\in\mathbf{I}$, $i\neq j$ 但 $a^i=a^j$.

命题 3 设 G 是个群, a 是 G 的元素. 则

$$\langle\{a\}\rangle=\{a^i\mid i\in\mathbf{I}\}.$$

证明 任取 G 的子群 H, $\{a\}\subseteq H$. 由于 H 是个群, $a\in H$, 则 $a^{-1}\in H$. 进而,对任意正整数 n, $a^n,(a^{-1})^n\in H$, 同时, $e=a^0\in H$. 总之,对任意整数 i 都有 $a^i\in H$.

由于 H 是任取的,所以 a^i 在所有这种子群 H 的交集里,也就是

$$a^i\in\langle\{a\}\rangle,\quad i\in\mathbf{I}.$$

即 $\{a^i\mid i\in\mathbf{I}\}\subseteq\langle\{a\}\rangle$.

另一方面,可以看出, G 的子集

$$H_0=\{a^i\mid i\in\mathbf{I}\}$$

是个子群. 因为 $a^i,a^j\in H_0$, 则

$$a^i(a^j)^{-1}=a^{i-j}\in H_0,$$

据定理 2, H_0 是 G 的子群. 而且 $\{a\}\subseteq H_0$.

但是，据定义，$\langle\{a\}\rangle$是 G 的所有包含子集$\langle\{a\}\rangle$的子群的交．上面说明 H_0 即这些子群里的一个，从而

$$\langle\{a\}\rangle\subseteq H_0.$$

最后得$\langle\{a\}\rangle=\{a^i \mid i\in\mathbf{I}\}$． ▍

当 S 是有限集，$S=\{g_1,\cdots,g_t\}$时，有时记$\langle S\rangle$为$\langle g_1,\cdots,g_t\rangle$．

例如，在正实数乘法群

$$\langle 2\rangle=\left\{\cdots,\frac{1}{4},\frac{1}{2},1,2,4,\cdots\right\},$$

这是个无限集合．

在$(\mathbf{I},+)$中，子群

$$\langle 2\rangle=\{\cdots-4,-2,0,2,4,\cdots\},$$

也有无穷个元素．

而在$(\mathbf{I}_6,+)$中，子群

$$\langle 2^*\rangle=\{0^*,2^*,4^*\}$$

只有 3 个元．因为 2^* 的各个整数倍（相应于乘法的乘方，这里称为倍）有些是重复的．

现在看两个元素 g,h 的集合$\{g,h\}$生成的子群$\langle g,h\rangle$．由于$\langle g,h\rangle$是个群，$g\in\langle g,h\rangle$，则

$$g^i\in\langle g,h\rangle,\quad i\in\mathbf{I},$$

由 $h\in\langle g,h\rangle$推出

$$h^i\in\langle g,h\rangle,\quad i\in\mathbf{I}.$$

进而，这两类元素的乘积

$$h^jg^i,g^ih^j\in\langle g,h\rangle,\quad i,j\in\mathbf{I}.$$

再进一步，上述 4 类元素的乘积也要在$\langle g,h\rangle$中．

一般地，G 中所有形如

$$g^ih^jg^th^s\cdots g^ph^q,\quad i,j,t,s,\cdots,p,q\in\mathbf{I}\qquad (*)$$

的元素都应属于$\langle g,h\rangle$．

要注意，表达式$(*)$中，有的 g 出现 3 次，有的可能出现 5 次，有的出现几千次，它代表了所有出现有限个 g,h 的情形，每个

表达式的长度不尽相同. 但取定一个表达式, 那么, g 和 h 在其中出现的次数是个固定的正整数, 或 3, 或 5 或几千, 等等.

这个表达似乎 g, h 的地位不对称, g 在前而 h 在后. 而实际上, 因为可以取 $i=0$,

$$g^0=e,$$

那么, 就有

$$g^0h^jg^th^s\cdots g^ph^q=h^jg^t\cdots h^qg^0.$$

可以验证, 所有(*)元素构成 G 的一个子群. 而这个验证工作包含在下面的更有普遍意义的定理 3 中.

设 S 是群 G 的一个非空子集, G 中所有形如

$$g_1^{t_1}g_2^{t_2}\cdots g_m^{t_m},\quad 0<m\in\mathbf{I},\ g_1,\cdots,g_m\in S,\ t_1,\cdots,t_m\in\mathbf{I}$$

的元素构成 G 的一个子集 H.

让我们先解释一下.

m 是个正整数. 取定一个 m 之后, 在 S 里取任意 m 个元素 $g_1,\cdots,g_m$, 这里允许重复, 即允许有 $i\neq j$, $0<i,j\leqslant m$, $g_i=g_j$.

然后, 任意取 m 个整数 $t_1,\cdots,t_m$, 得一个元素

$$g_1^{t_1}g_2^{t_2}\cdots g_m^{t_m}.$$

定理 3 符号如上所述, 则 $\langle S\rangle=H$.

证明 先来证明 H 是 G 的子群.

S 非空, 设 $g\in G$, $g\in S$. 取 $m=1$, $g\in S$, $t_1=1$, 则元素 $g^1=g\in H$, 故 H 非空.

从这里也看出, $S\subseteq H$.

任取 H 中的两个元素, 即任取正整数 m,n, 再任取 $g_1,\cdots,g_m\in S$, $h_1,\cdots,h_n\in S$, 又取整数 $t_1,\cdots,t_m$ 和 $l_1,\cdots,l_n$, 得

$$g=g_1^{t_1}g_2^{t_2}\cdots g_m^{t_m}\in H,\quad h=h_1^{l_1}h_2^{l_2}\cdots h_n^{l_n}\in H.$$

它们的乘积

$$gh=g_1^{t_1}\cdots g_m^{t_m}h_1^{l_1}\cdots h_n^{l_n}$$

仍然具有 H 所要求的形式，也就是 $gh\in H$.

对任意

$$g=g_1^{t_1}\cdots g_m^{t_m}\in H,$$

元素

$$g^{-1}=g_m^{-t_m}\cdots g_1^{-t_1}$$

也具有 H 所要求的形式，故 $g^{-1}\in H$.

据定理 1, H 是 G 的一个子群.

刚刚证过，$S\subseteq H$. 于是，据 $\langle S\rangle$ 的定义，它是 G 中所有包含 S 的子群的交集，而 H 为这些群中的一个，故有 $\langle S\rangle\subseteq H$.

反过来，设 K 是 G 的一个包含集合 S 的子群. 对 H 中的任意元

$$g=g_1^{t_1}\cdots g_m^{t_m},\quad g_1,\cdots,g_m\in S,$$

由 $g_i\in S\subseteq K$, K 是子群，知道 $g_i^{t_i}\in K$. 再进一步，它们的乘积

$$g=g_1^{t_1}\cdots g_m^{t_m}\in K.$$

所以，$H\subseteq K$, $H\subseteq\langle S\rangle$.

最后证得 $H=\langle S\rangle$. ∎

例题 4 设 G 是个群，H 是由元素 a,b 生成的子群，且 $ab=b^2a$, $ba=a^2b$. 证明：H 是 G 的由恒等元 e 生成的子群（平凡子群）.

证明 由于

$$ab=b^2a=b(ba)=ba^2b,$$

从右端消去 b 得 $a=ba^2$；再从右端消去 a 得 $e=ba$. 于是知道 $ab=ba=e$. 进一步，由于

$$b=b(ba)=b^2a=ab=e,$$

$$a=a^2b=a(ab)=ba=e,$$

即知 $a=b=e$, $\langle a,b\rangle=H=\langle e\rangle$. ∎

例题 5 设 H 是所有 3 阶实的非奇异矩阵在矩阵乘法之下

构成的群(看例题 1).而 K 是所有形如

$$\begin{pmatrix}1 & a & b\\0 & 1 & c\\0 & 0 & 1\end{pmatrix},\quad a,b,c\in \mathbf{I}$$

矩阵的集合.这种矩阵均为非奇异的,从而 K 是 H 的子集.进一步,证明:K 是 H 的子群.

证明 任取整数 a,b,c,d,e,f,有

$$\begin{pmatrix}1 & a & b\\0 & 1 & c\\0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & d & e\\0 & 1 & f\\0 & 0 & 1\end{pmatrix}=\begin{pmatrix}1 & d+a & e+af+b\\0 & 1 & f+c\\0 & 0 & 1\end{pmatrix}\in K.$$

而对任意

$$X=\begin{pmatrix}1 & a & b\\0 & 1 & c\\0 & 0 & 1\end{pmatrix},$$

观察刚刚计算过的等式,取

$$d=-a,\quad f=-c,\quad e=ac-b,$$

即有

$$\begin{pmatrix}1 & a & b\\0 & 1 & c\\0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & -a & ac-b\\0 & 1 & -c\\0 & 0 & 1\end{pmatrix}=\begin{pmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix},$$

也就是说矩阵 X 的逆

$$\begin{pmatrix}1 & -a & ac-b\\0 & 1 & -c\\0 & 0 & 1\end{pmatrix}\in K,$$

所以,K 是 H 的子群. ▌

例题 6 在上面例题 5 给出的群 K 中分别计算,由矩阵

$$X=\begin{pmatrix}1 & 1 & 0\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix},\quad Y=\begin{pmatrix}1 & 0 & 1\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix},\quad Z=\begin{pmatrix}1 & 0 & 0\\0 & 1 & 1\\0 & 0 & 1\end{pmatrix}$$

生成的子群$\langle X\rangle$,$\langle Y\rangle$,$\langle X,Y,Z\rangle$,$\langle X,Z\rangle$.

解 前面已经分析过元素 X 在 K 中生成的子群乃是由 X 的各种方次 X^n 组成,$n\in \mathrm{I}$. 现在,我们来具体的计算出 X^n. 实际上,对任意 $n\geqslant 1$,有

$$\begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}^n=\begin{pmatrix}1 & n & 0\\ 0 & 1 & 0\\ 0 & 1 & 1\end{pmatrix}.$$

可以对 n 用数学归纳法. $n=1$ 时断言正确. 如果断言对 n 的情形正确,那么

$$X^{n+1}=X^n\cdot X=\begin{pmatrix}1 & n & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}=\begin{pmatrix}1 & n+1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}.$$

当 n 为负正数时,设 $n=-m$,则 $m\geqslant 1$,于是

$$X^n=X^{-m}=(X^{-1})^m=\begin{pmatrix}1 & -1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}^m=\begin{pmatrix}1 & n & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix},$$

所以,

$$\langle X\rangle=\left\{\begin{pmatrix}1 & n & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}\middle|\, n\in \mathrm{I}\right\}.$$

同理可以算出

$$\langle Y\rangle=\left\{\begin{pmatrix}1 & 0 & n\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}\middle|\, n\in \mathrm{I}\right\}.$$

要搞清 X,Z 两个元素在 K 中生成的子群$\langle X,Z\rangle$的结构,先注意

$$XZ=\begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 1\\ 0 & 0 & 1\end{pmatrix}=\begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 1\\ 0 & 0 & 1\end{pmatrix}=ZX,$$

所以$\langle X,Z\rangle$中一般元素必形如X^nZ^m，其中m和n是任意整数，而X^n与Z^m我们已计算过了，故

$$\langle X,Z\rangle=\left\{\begin{pmatrix}1&n&0\\0&1&m\\0&0&1\end{pmatrix}\middle|\, m,n\in\mathbf{I}\right\}.$$

最后，我们看子群$\langle X,Y,Z\rangle$. 本来应该研究X^m,Y^n,Z^l各种可能的乘积

$$X^mY^mZ^lX^kY^jZ,\quad X^mY^nZ^lX^kY^jZ^iX^rY^t,$$

等等.

但是，熟悉线性代数中初等变换方法的人容易看出（不能马上看出也不影响本课程的学习）

$$\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}=\begin{pmatrix}1&a&0\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&b\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&b-ac\\0&1&0\\0&0&1\end{pmatrix},$$

也就是说，在K中，对任意$a,b,c\in\mathbf{I}$，有

$$\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}=X^aZ^cY^{b-ac},$$

所以$\langle X,Y,Z\rangle=K$. ∎

对任意群G而言，G本身是G的一个子群；单独一个恒等元e也构成一个子群$\{e\}$；这2个子群称为G的平凡子群.

习 题 二

1. 用i代表纯虚数. 证明：$\{1,-1,\mathrm{i},-\mathrm{i}\}$是所有非零有理数乘法群的一个子群.

2. 设a是群G的一个固定元素. 证明：$H=\{g\in G\mid ga=ag\}$是G的一个子群.

3. 所有形如

$$\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\quad(a,b,c\text{ 是偶数})$$

的矩阵的集合 E 是例题 5 中群 K 的一个子群.

4. 如果 G 是个交换群，m 是个正整数，那么 $H=\{g\in G \mid g^m=e\}$ 是 G 的一个子群.

5. 所有的非零有理数的集合在数的乘法之下构成的群记为 $\mathbf{Q}^*$. 证明：所有的正的有理数的集合 P 是 $\mathbf{Q}^*$ 的一个子群.

6. 在有理数集 $\mathbf{Q}$ 与集 $\mathbf{Q}-\{0\}$ 的笛卡尔积

$$G=(\mathbf{Q}-\{0\})\times\mathbf{Q}$$

上规定，对任意 $(a,b)\in G$，$(c,d)\in G$，

$$(a,b)\Delta(c,d)=(ac,bc+d).$$

证明：(G,Δ) 是个群. 再证明：G 中所有形如

$$(1,b),\quad b\in\mathbf{Q}$$

的元素的集合 H 是 G 的一个子群.

7. 在所有复的可逆 2 阶矩阵构成的乘法群中，矩阵

$$I=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\ A=\begin{pmatrix}\mathrm{i} & 0\\ 0 & -\mathrm{i}\end{pmatrix},\ B=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\ C=\begin{pmatrix}0 & \mathrm{i}\\ \mathrm{i} & 0\end{pmatrix},$$

$$-I=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix},\ -A=\begin{pmatrix}-\mathrm{i} & 0\\ 0 & \mathrm{i}\end{pmatrix},\ -B=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix},\ -C=\begin{pmatrix}0 & -\mathrm{i}\\ -\mathrm{i} & 0\end{pmatrix}.$$

构成一个子群(此群称为**克莱因(Klein)四元数群**).

§3 对称群与置换群

群的初等理论中相当多的问题来自于几何学，特别是来自对称性的讨论.

时至今日，群论最活跃的几个领域中，如平面或空间运动、晶体结构、生物遗传等，群的威力仍主要体现在处理各式各样的对称问题上.

在第一章 §5，我们实际上证明了，集合

$$\mathbf{S}=\{1,2,\cdots,n\}$$

上所有置换在映射合成之下构成群. 今后称这个群为 **n 次对称群**，记为 $\mathbf{S}_n$. 同时，实际上，我们也证明了，$\mathbf{S}$ 上的所有偶置换，在映

射的合成之下也构成群，这是 S_n 的一个最重要的子群，通常记为 A_n，称为 n **次交代群**.

定义 1 n 阶对称群 S_n 的任意一个子群都称为是个**置换群**.

例 1 在对称群 S_3 中，令

$$P_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad P_4=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},$$

$$P_2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\quad P_5=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},$$

$$P_3=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\quad P_6=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}.$$

那么，S_3 的乘法表是

$\circ$	P_1	P_2	P_3	P_4	P_5	P_6
P_1	P_1	P_2	P_3	P_4	P_5	P_6
P_2	P_2	P_1	P_6	P_5	P_4	P_3
P_3	P_3	P_5	P_1	P_6	P_2	P_4
P_4	P_4	P_6	P_5	P_1	P_3	P_2
P_5	P_5	P_3	P_4	P_2	P_6	P_1
P_6	P_6	P_4	P_2	P_3	P_1	P_5

乘的顺序是先从左侧竖列中取一置换 P_i，再在上行中取一置换 P_j，交叉路口得的是 $P_i\circ P_j$.

命题 1 当 $n\geqslant 3$ 时，S_n 不是可交换的.

证明 设

$$P=\begin{pmatrix}1&2&3&\cdots\\1&3&2&\cdots\end{pmatrix},\quad Q=\begin{pmatrix}1&2&3&\cdots\\3&2&1&\cdots\end{pmatrix},$$

其中 3 以后的数字在 P 和 Q 之下都从自己变到自己. 于是

$$Q\circ P=\begin{pmatrix}1&2&3&\cdots\\3&1&2&\cdots\end{pmatrix},\quad P\circ Q=\begin{pmatrix}1&2&3&\cdots\\2&3&1&\cdots\end{pmatrix},$$

即 $Q\circ P\neq P\circ Q$，S_n 不是交换群. ∎

对于 S_3，我们从其乘法表上即可看出它不是交换群，因为

$$P_2 \circ P_5 = P_4, \quad P_5 \circ P_2 = P_3.$$

但是对于数目较大的 n，给出其乘法表亦不是一件简单的工作.但对于一般 S_n 的性质的讨论有时可以从 S_3 的乘法表中受到启发.

对于 S_3，从乘法表上就可以找出其全部子群，也就是$\{1,2,3\}$上的所有置换群.

首先是$\{P_1\}$和 S_3 自己.其次是$\{P_1, P_2\}$，$\{P_1, P_3\}$，$\{P_1, P_4\}$，因为

$$P_2^2 = P_1, \quad P_3^2 = P_1, \quad P_4^2 = P_1,$$

也就是 $P_2^{-1} = P_2$，$P_3^{-1} = P_3$，$P_4^{-1} = P_4$，从而

$$\langle P_2 \rangle = \{P_1, P_2\}, \quad \langle P_3 \rangle = \{P_1, P_3\}, \quad \langle P_4 \rangle = \{P_1, P_4\}.$$

再次是$\{P_1, P_5, P_6\}$，因为

$$P_5 \circ P_6 = P_6 \circ P_5 = P_1, \quad P_5^2 = P_6, \quad P_6^2 = P_5.$$

后面，我们会有相当方便的办法来判断，S_3 的于群只有这些.

为了更深入了解 n 阶置换的特性，常常把它们表示成所谓"循环"的乘积.

定义 2 如果 n 阶置换 P，把 1 到 n 中若干个数码 $i_1, i_2, \cdots, i_k$ 按下方式对应

$$P(i_1) = i_2, \quad P(i_2) = i_3, \cdots, \quad P(i_k) = i_1,$$

而对其余数码 x，有 $P(x) = x$，则说 P 是一个 k **循环**，记

$$P = (i_1\ i_2 \cdots\ i_k).$$

当然，一个循环 P 的记法不只一种方式，例如，

$$(i_1\ i_2 \cdots\ i_k) = (i_2 \cdots\ i_k\ i_1)$$

因为它们代表相同的映射.

例 2 在 S_6 中

$$(1\ 2\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix},$$

$$(6\ 3\ 4\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 4 & 2 & 5 & 3 \end{pmatrix}.$$

由于恒等置换可用不同的数字记出，即

$$\begin{pmatrix}1 & 2 & \cdots & n\\ 1 & 2 & \cdots & n\end{pmatrix}=(1)=(2)=\cdots,$$

以下所提到的循环均将其排除在外，也就是说，各循环均指 k 循环，$k\geqslant 2$ 者.

定义 3 循环$(i_1\ i_2\cdots\ i_k)$与$(j_1\ j_2\cdots\ j_k)$称之为**不交的**，如果

$$i_t\neq j_s\quad t=1,\cdots,k,\ s=1,\cdots,l.$$

命题 2 若$(i_1\ i_2\cdots\ i_k)$与$(j_1\ j_2\cdots\ j_l)$不交，则它们可交换.

证明 由于 $i_1,\cdots,i_k$ 和$j_1,\cdots,j_l$ 都是从 1 到 n 之间的数码，且两两不同. 这两个映射无论按何种次序复合，其结果都是

$$\begin{pmatrix}i_1 & i_2 & \cdots & i_k & j_1 & j_2 & \cdots & j_l & \cdots\\ i_2 & i_3 & \cdots & i_1 & j_2 & j_3 & \cdots & j_1 & \cdots\end{pmatrix}.$$ ▌

定理 1 在 $\mathbf{S}_n$ 中，任何一个不等于恒等映射的置换必可表成若干个互不相交的循环的乘积.

证明 任取 $P\in\mathbf{S}_n$，$P\neq i_{\mathbf{S}_n}$. 那么，必有 $i\in\mathbf{S}_n$ 使 $P(i)\neq i$. 考虑序列

$$i,P(i),P^2(i),\cdots.$$

由于 $\mathbf{S}_n$ 只有 n 个不同的数码，上面的序列必然使有些数码重复出现. 设 $P^k(i)$是第一个与其前某个数码相同者. 也就是说，有 $l<k$ 且

$$P^l(i)=P^k(i),\tag{1}$$

而且 k 是出现这种重复的最小的数.

现在可以断言，$l=0$. 若不然，$l>0$，由于 P 是可逆映射. 将(1)式两端乘$(P^{-1})^l$ 得

$$i=P^{k-l}(i),$$

与 k 选择的最小性矛盾. 由于 $P^0(i),P(i),\cdots,P^{k-1}(i)$两两不同，故知 $k\leqslant n$.

这就是说

$$i, P(i), \cdots, P^{k-1}(i) \tag{2}$$

两两不同，且 $P(P^{k-1}(i)) = P^k(i) = i$. 由于 P 可以用任何方式写出，我们把(2)排在前面，得

$$P = \begin{pmatrix} i & P(i) & \cdots & P^{k-1}(i) & \cdots \\ P(i) & P^2(i) & \cdots & i & \cdots \end{pmatrix}.$$

如果 $k = n$，则 P 即为一个 n 循环，定理证毕. 如果 $k < n$，即有数码 $1 \leqslant j \leqslant n$，$j$ 没有出现在(2)中.

这些在(2)中没曾出现的数码 j 如果都有

$$P(j) = j,$$

那么，P 即为 k 循环，$P = (i\ P(i)\ \cdots\ P^{k-1}(i))$.

如果有 j 没出现在(2)中，而且 $P(j) \neq j$，由于 P 有逆，$P(j)$ 也不会出现在(2)中，进而序列

$$j, P(j), P^2(j), \cdots \tag{3}$$

中任何数码均不在(2)中.

于是，将(3)作上面对(2)刚刚作过的分析，可得一个整数 t，使

$$j, P(j), \cdots, P^{t-1}(j)$$

两两不同，且它们与(2)中数码完全不同，同时还有

$$P(P^{t-1}(j)) = P^t(j) = j.$$

这样，又可将 P 写成

$$P = \begin{pmatrix} i & P(i) & \cdots & P^{k-1}(i) & j & P(j) & \cdots & P^{t-1}(j) & \cdots \\ P(i) & P^2(i) & \cdots & i & P(j) & P^2(j) & \cdots & P^t(j) & \cdots \end{pmatrix}.$$

由于 $\mathbf{S}_n$ 只有 n 个数码，经过有限步骤，最后 P 按这种分段方式写出来，也就得

$$P = (i\ P(i)\ \cdots\ P^{k-1}(i)) \cdots (m\ P(m)\ \cdots\ P^{r-1}(m)),$$

这些循环两两不交. ∎

例 3 把下面的 9 阶置换写成轮换乘积

$$A=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 7 & 3 & 2 & 8 & 5 & 4 & 9 & 6 & 1\end{pmatrix}.$$

先从 1 开始看,有

$$1\to7\to9\to1.$$

再看 2,又有

$$2\to3\to2.$$

接着看 4,乃是

$$4\to8\to6\to4.$$

最后剩下一个 5,所以

$$A=(5)(4\ 8\ 6)(2\ 3)(1\ 7\ 9).$$

如果你从 6 开始,得(6 4 8);再得(5);接着看 7 得(7 9 1);最后看 3 得(3 2).那么 A 又可写成

$$A=(3\ 2)(7\ 9\ 1)(5)(6\ 4\ 8).$$

上述两乘积表达式中之 1 循环可以不写.

下面我们讨论所谓分解的唯一性问题,准确地说,有

定理 2 设 P 是个 n 置换,

$$P=P_1\cdots P_l=Q_1\cdots Q_k,\tag{4}$$

其中 $P_1,\cdots,P_l$ 是两两不相交的循环,$Q_1,\cdots,Q_k$ 亦为两两不相交的循环.那么,必有 $k=l$,且可将诸 Q_i 的顺序适当调整,使得

$$P_1=Q_1,\cdots,P_k=Q_k.$$

我们已经声明过,此处循环不包括 1 循环在内.

证明 设

$$P_1=(a_1\ a_2\ \cdots\ a_m).$$

由于 $P(a_1)=a_2\neq a_1$,a_1 必然出现在某一个 Q_j 中.将 Q_i 顺序调整,Q_j 排到最前.由于它们是两两不交的循环,其乘积交换顺序后仍为 P.也就是说,现在不妨就假定 Q_1 中出现 a_1.

由于循环中出现的数字可以以其中任意一个数码为首,故可设

$$Q_1=(a_1\ b_2\ \cdots\ b_l).$$

但 P_1 告诉我们,$P(a_1)=a_2,\cdots,P(a_m)=a_1$,所以在 Q_1 中相应有

$$P(a_1)=b_2,\ \cdots,\ P(b_l)=a_1,$$

也就是 $a_2=b_2,\ \cdots,\ b_l=a_m$(当然也说明了 $m=l$),即 $P_1=Q_1$.

将(4)式两端同乘 P_1^{-1},得

$$P_2\cdots P_l=Q_2\cdots Q_k.$$

经调整顺序,同上一样可有 $P_2=Q_2$,再消去它们.

如此继续下去,经过有限步,即知 $l=k$.且

$$P_1=Q_1,\quad \cdots,\quad P_k=Q_k.$$ ∎

命题 3 任意一个 k 循环都可以表成若干个 2 循环的乘积.

证明 用数学归纳法证明

$$(i_1\ i_2\ \cdots\ i_k)=(i_k\ i_1)\cdots(i_1\ i_3)(i_1\ i_2).$$

当 $k=2$ 时,命题正确.

如果已经知道

$$(i_1\ i_2\ \cdots\ i_{k-1})=(i_1\ i_{k-1})\cdots(i_1\ i_2),$$

那么,作为映射,

$$(i_1\ i_k)(i_1\ i_2\ \cdots\ i_{k-1})=(i_1\ i_k)(i_1\ i_{k-1})\cdots(i_1\ i_2).$$

把 i_2 变成 i_3,把 i_3 变成 i_4……把 i_{k-1}经由 i_1 变成 i_k, i_k 变成i_1,且把 i_1 变成 i_k,也就是

$$\begin{aligned}(i_1\ i_k)(i_1\ i_2\ \cdots\ i_{k-1})&=(i_1\ i_k)\cdots(i_1\ i_2)\\&=(i_1\ i_2\ \cdots\ i_{k-1}\ i_k).\end{aligned}$$ ∎

例 4 在 S_5 中,有

$$\begin{pmatrix}1&2&3&4&5\\3&4&1&5&2\end{pmatrix}=(1\ 3)(2\ 4\ 5),$$

$$(1\ 4\ 5)(2\ 3\ 5)=(1\ 4\ 5\ 2\ 3),$$

$$(1\ 5)(1\ 4)(1\ 3)(1\ 2)=(1\ 2\ 3\ 4\ 5),$$

$$(1\ 2\ 3\ 4)^{-1}=(4\ 3\ 2\ 1)=(1\ 4\ 3\ 2).$$

命题 4 在 S_n 中，k 循环 P 生成的子群是

$$\langle P\rangle=\{i_s, P, \cdots, P^{k-1}\}.$$

事实上，$P^k=i_{s_n}$，而当 $i<k$ 时，$P^i\neq i_{s_n}$，故元素

$$i_{s_n}, P, \cdots, P^{k-1} \tag{5}$$

两两不同，而对其中任意一个元素之任意方幂，

$$(P^i)^j,\quad 0\leqslant i\leqslant k-1$$

用 k 除 ij 可得

$$ij=qk+r,\quad 0\leqslant r<k,$$

即知 P^{ij} 是(5)中的一个. ▌

再来讨论一个置换群的子群.

命题 5 设 $S=\{1,2,\cdots,n\}$，G 是 S 上的一个置换群. 对于 S 的任意一个子集 T，令

$$G_T=\{P\in G\mid P(t)=t, \text{对每个 } t\in T\}.$$

则 G_T 是 G 的一个子群.

证明 单位置换 i_S 使得 S 的所有元素不变，当然有 $i_S\in G_T$，即 G_T 非空.

如果 $P, Q\in G_T$，那么，对任意 $t\in T$ 都有

$$P(t)=t,\quad Q(t)=t,$$

从而 $(PQ)(t)=P(Q(t))=t$，即 $PQ\in G_t$.

如果 $P\in G_T$，那么，对任意 $t\in T$，都有

$$P(t)=t,$$

两端都用 P^{-1} 作用之，得 $P^{-1}(t)=P^{-1}(P(t))=(P^{-1}P)(t)=t$. 也就是

$$P^{-1}\in G_T.$$

从而 G_T 为 G 的子群. ▌

命题 6 设 $S=\{1,2,\cdots,n\}$，G 是 S 上的一个置换群，T 是 S 的一个子集. 令

$$G^T=\{P\in G\mid P(T)\subseteq T\},$$

则 G^T 是 G 的一个子群.

证明 恒等置换 $i_S\in G^T$,故 G^T 非空.

如果 $P,Q\in G^T$,即

$$P(T)\subseteq T,\quad Q(T)\subseteq T,$$

从而

$$(PQ)(T)\subseteq P(Q(T))\subseteq P(T)\subseteq T.$$

也就是 $PQ\in G^T$.

最后,若 $P\in G^T$,即 $P(T)\subseteq T$,那么,由于 P 是置换,是单射,T 中不同的元素在 $P(T)$ 中对应不同的元素.假设 T 有 m 个元素,那么,$P(T)$ 元素个数不少于 m 个,但 $P(T)$ 又在 T 中,这就意味着 $P(T)=T$.于是

$$P^{-1}(P(T))=P^{-1}(T)=T.$$

这说明 $P^{-1}\in G^T$.

总之,G^T 为 G 的子群. ∎

命题 5 和命题 6 中所给出的置换群 G 的两类重要子群.显然,对同一个子集 T,有

$$G_T\subseteq G^T,$$

G_T 是 G^T 的子群,G_T 中的置换使得 t 之每个元素都不动,而 G^T 中的置换使 T 中元素只在 T 中变.通常,因 G_T 保持 T 中元素不动,而称 T 是对 G_T 的对称轴,G_T 是研究对称性的一个重要概念.

现在,用一简单例题说明置换与对称性的联系.与所有的例题一样,只是要求读者通过它加深对本节正文的理解而不要求大家记住例题中的名词和结论.

例题 1 设有等边三角形,其顶点记为 1,2,3.我们研究在 3 维几何空间能使该三角形与自己重合的所有刚性变换.所谓刚性变换即保持空间任意两点距离不变的映射.

因此，一个三角形在一个刚性变换之下的变化可由其 3 个顶点的变化完全决定.

用 S_3 中的 6 个置换就全部地描写了使这个三角形与自己重合的变换.

先看这个的刚体变换，它们仅仅是使得该三角形发生了旋转. 对照例 1，有图 2－2.

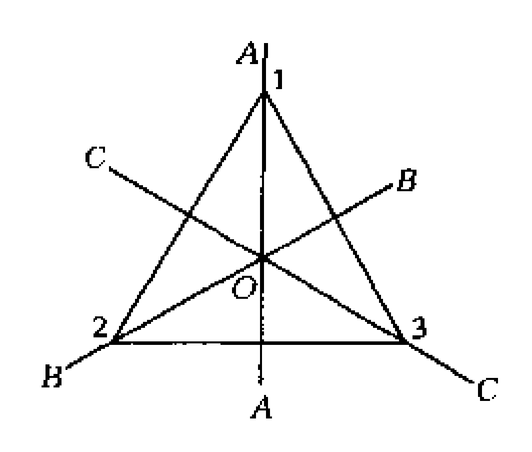


图 2－1

因为 P_1，P_5 和 P_6 都是旋转

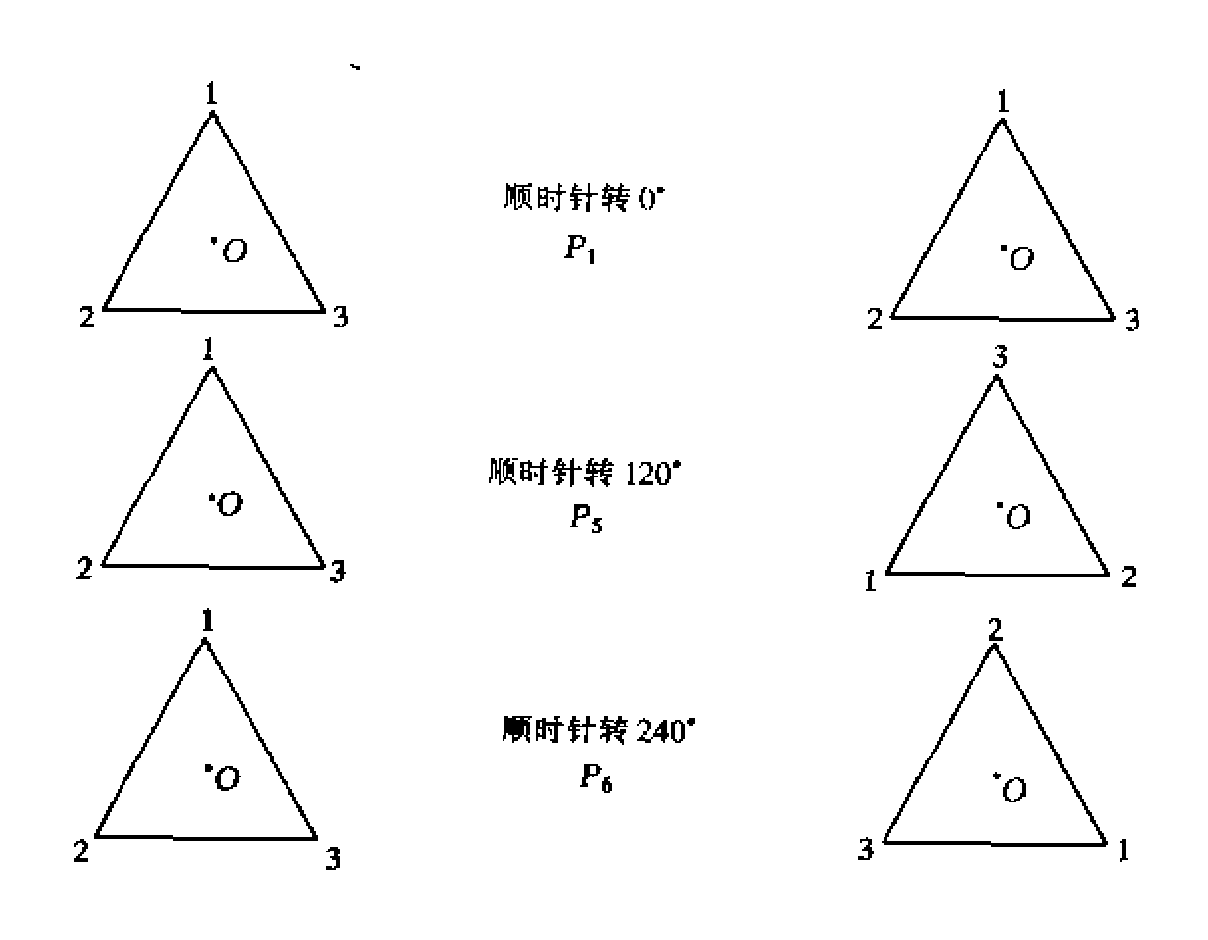


图 2－2

变换，复合后仍为旋转变换，所以

$$\{P_1, P_5, P_6\}$$

是 S_3 的一个子群.其乘法表是很容易算的,

$\circ$	P_1	P_5	P_6
P_1	P_1	P_5	P_6
P_5	P_5	P_6	P_1
P_6	P_6	P_1	P_5

再来看三角形按轴 AA, BB 和 CC 的 3 个翻转变换,三角形翻转了 180°,仍然与原三角形重合.

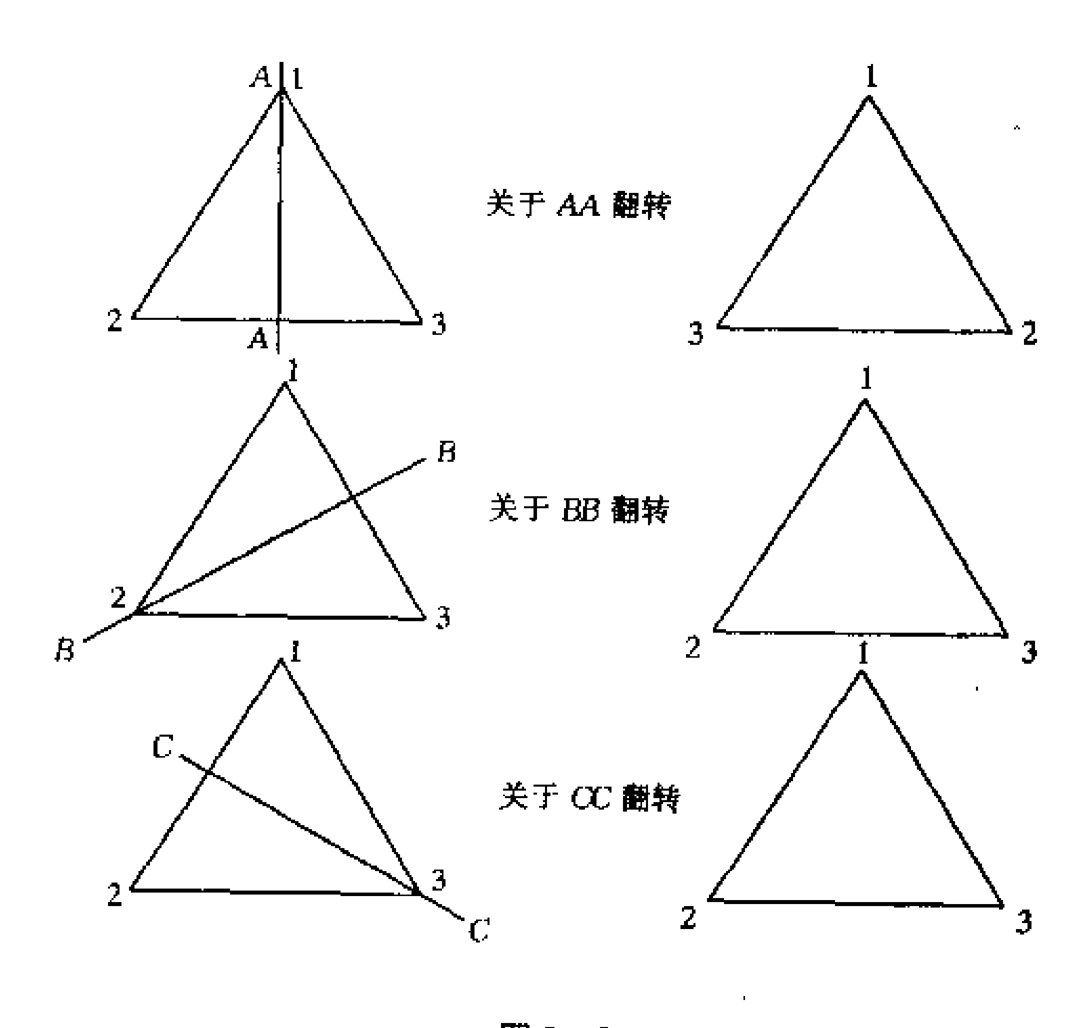


图 2－3

顶点的变化恰如例 1 中给出的 $\mathbf{S}_3$ 中的置换 P_4, P_5 和 P_6.

关于 AA 翻转 2 次，得 $P_4 \circ P_4 = P_1$，又恢复原状态. $\{P_1, P_4\}, \{P_1, P_5\}, \{P_1, P_6\}$分别为 $\mathbf{S}_3$ 的子群.

进一步，可以看出，两个关于不同轴的翻转合成后是旋转.

如果 $\mathbf{S}_3$ 的一个子群 G 含有映射 P_2 和 P_3，那么，G 就含有它们的合成 P_5 和 P_6. 而 P_2P_5 和 P_2P_6 不等且都不等于 P_2，它们之中必然有一个是 P_4，所以 G 必然含有 P_4，也就是说 G 必然等于 $\mathbf{S}_3$.

对于含 P_2, P_4 或含 P_3, P_4 的子群，相应地，也可知道它们必为 $\mathbf{S}_3$. ▮

为了熟悉置换群中的运算性质，再看

例题 2 在对称群 $\mathbf{S}_8$ 中，求元素

$$A = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8),$$
$$B = (1\ 5\ 3\ 7)(2\ 8\ 6\ 4)$$

生成的子群.

解 首先 A, B 生成的子群必含 A, B 的方幂，计算之，

$$A^2 = (1\ 3)(2\ 4)(5\ 7)(6\ 8),$$
$$A^3 = (1\ 4\ 3\ 2)(5\ 8\ 7\ 6),$$

而 A^4 是两个独立的 4 循环的 4 次方，由命题 4 知每个 4 循环的 4 次方都等于恒等置换，即 $A^4 = (1)$.

同样可算出

$$B^2 = (1\ 3)(5\ 7)(2\ 4)(6\ 8),$$
$$B^3 = (1\ 7\ 3\ 5)(2\ 6\ 4\ 8),$$
$$B^4 = (1).$$

进一步，$\langle A, B\rangle$还应包含

$$AB = (1\ 6\ 3\ 8)(2\ 5\ 4\ 7),$$
$$BA = (1\ 8\ 3\ 6)(2\ 7\ 4\ 5).$$

注意到 $A^2 = B^2$，我们已经算出子群$\langle A, B\rangle$中的 8 个不同的

元素,即一个“字母”的 A, B,两个字母的 $AA=BB, AB, BA$,且二字母只有以上 4 种情形.对于三字母,已算出 AAA 和 BBB.同时,因为 $A^2B=B^3$, $BA^2=B^3$, $B^2A=A^3$, $AB^2=A^3$,知道另外 4 个三字母元也已经出现过了.

现在计算

$$ABA=(1\ 5\ 3\ 7)(2\ 8\ 4\ 6)=B,$$

$$BAB=(1\ 2\ 3\ 4)(5\ 6\ 7\ 8)=A.$$

对于四字母情形,由于 $A^2=B^2$,从而

$$ABBA=AAAA, \quad BAAB=BBBB.$$

进而,任意 4 个字母情形,必然是 3 个相同字母相连,或者两同字母夹另一字母,如

$$ABAX, \quad YBAB.$$

这两种情形都可化简,如

$$ABAX=BX, \quad YBAB=YA,$$

$$AAAB=B^2AB=B(BAB)=BA,$$

总之,四字母者必可化短.

更长的多字母情形一定可逐步化短为三字母以下情形.所以,前面给出的 8 个不同置换就是子群 $\langle A, B\rangle$ 的全部元素. ▌

习 题 三

1. 在 S_4 中求出 $\langle(1\ 2\ 3\ 4)\rangle$, $\langle(1\ 2), (3\ 4)\rangle$ 的元素.
2. 给出 4 阶交代群的元素(即所有 4 阶偶置换).
3. 在 S_4 中求子群

$$H=\{P\in S_4 \mid P(1)=1,\ P(2)=2\},$$

$$K=\{P\in S_4 \mid P(\{1,2\})\subseteq\{1,2\}\}.$$

4. 在 S_5 中,把下列置换表成不相交的轮换之积:

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 4 & 1 & 5 & 2\end{pmatrix},$$

$$(2\ 4)(1\ 3\ 2)(2\ 5\ 4).$$

$$(1\ 5)(1\ 4)(1\ 3)(1\ 2),$$
$$(1\ 2\ 3\ 4\ 5)^{-1}.$$

5*. 看 $\mathbf{R}^4$ 到 $\mathbf{R}$ 的映射(即一个四元函数)

$$f(x_1,x_2,x_3,x_4)=x_1x_2+x_3+x_4$$

再把 $\mathbf{S}_4$ 中的置换 σ 写成

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) \end{pmatrix}.$$

证明:$\mathbf{S}_4$ 中所有使得 f 不变的 σ,即

$$f(x_{\sigma(1)},x_{\sigma(2)},x_{\sigma(3)},x_{\sigma(4)})=f(x_1,x_2,x_3,x_4)$$

构成 $\mathbf{S}_4$ 的一个子群,并把它的所有元素写出来.

§4 循 环 群

在讨论群 G 的子集 S 生成的子群时,我们已经看出,当 S 只含一个元素 a 时,它生成的子群 $\langle\{a\}\rangle=\langle a\rangle$ 表达起来相当简单,其元素间运算也十分明了.

进一步学习群论还会发现,有一些地位相当重要的群,实际上,可由这种由单个元素生成的子群"拼凑"而成.

定义 1 群 G 称为**循环群**,如果有 $g\in G$,使得 $G=\langle g\rangle$. 也有人称循环群为巡回群.

例 1 在 $\mathbf{S}_4$ 中,考虑置换

$$g=(1\ 2\ 3\ 4),\quad g^2=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix},$$
$$g^3=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix},\quad g^0=g^4=i.$$

这 4 个置换构成 $\mathbf{S}_4$ 的一个子群 $G=\langle g\rangle$.

例 2 整数集 $\mathbf{I}$ 上所有双射,在映射的合成之下构成群 $S_{\mathbf{I}}$. 映射 $g:\mathbf{I}\to\mathbf{I}$,

$$g(i)=i+1,\quad 对每个\ i\in\mathbf{I},$$

生成的子群 $\langle g\rangle$ 中,任意一个元素 g^k 必使得

$$g^k(i)=k+i,\quad \text{对每个 } i\in \mathbf{I}.$$

这说明,当而且仅当 $k=l$ 时,$g^k=g^l$.所以

$$\langle g\rangle=\{\cdots,g^{-1},i_1,g,g^2,\cdots\}.$$

从例子中,可以看出,一个循环群的生成裕 α 是唯一的,例 1 中

$$G=\langle g\rangle=\langle g^3\rangle.$$

例 2 中也有$\langle g\rangle=\langle g^{-1}\rangle$.下面要说明,所说的不唯一,不仅仅是对任何 $g\in G$ 而言,都有$\langle g\rangle=\langle g^{-1}\rangle$,而且有更一般地判断元素是否为生成元的办法.

命题 1 设 G 是个群,$g\in G$.如果有不同的整数 r 和 k 使得 $g^r=g^k$,则存在一个正整数 m 使得

(1) $g^m=e$, e 是 G 的恒等元;

(2) 当 $1\leqslant i<j\leqslant m$ 时,$g^i\neq g^j$;

(3) 如果有整数 t, $g^t=e$,则 $m\mid t$;

(4) $\langle g\rangle=\{e,g,g^2,\cdots,g^{m-1}\}$.

证明 不妨假定 $r>k$.由 $g^r=g^k$,两端乘 g^{-k},得 $g^{r-k}=e$.这说明,一定有正整数 t 使得 $g^t=e$.

设 m 是正整数集

$$M=\{t\in\mathbf{I}\mid g^t=e \text{ 且 } t>0\}$$

中的最小者.于是首先有 $g^m=e$.

其次,对 $1\leqslant i<j\leqslant m$,由 $j-i<m$ 和 m 的极小性可知 $g^{j-i}\neq e$,从而 $g^j\neq g^i$.

再次,对任意 $t\in\mathbf{I}$,如果 $g^t=e$,作除法,得

$$t=mq+l,\quad 0\leqslant l<m.$$

则应有 $g^t=g^{mq}g^l$, $(g^m)^q=e^q=e$.故

$$g^l=g^{mq}g^l=g^t=e.$$

而 m 是M 中最小者,故 $l\notin M$, $l=0$,也就是 $m\mid t$.

最后,形式上,$\langle g\rangle$应包含 g 的任意次幂g^n, $n\in\mathbf{I}$.但是,正如上面作过的,我们能够得到

$$n = mp + h, \quad 0 \leqslant h < m, \ p \in \mathbf{I}.$$

使 $g^n = g^h$；从而

$$g^n \in \{e, g, g^2, \cdots, g^{m-1}\},$$

这就证明了(4)，也完成了整个命题的证明. ▌

命题 2 设 G 是个群，$g \in G$. 如果对任意不同的整数 r, k 都有 $g^r \neq g^k$，则 $\langle g \rangle$ 是个无限群(即有无限多个元素).

事实上，$\langle g \rangle$ 中的每个元素的形式均为 g^n，n 是整数，由所设条件，元素

$$\cdots g^{-1}, e, g, g^2, \cdots$$

两两不同，故循环群

$$\langle g \rangle = \{\cdots, g^{-1}, e, g, g^2, \cdots\}$$

含无限多个元素. ▌

特别地，对于循环群，我们有

定理 1 设 g 是循环群 G 的一生成元，那么

(1) 当有正整数 $r \neq k$，使 $g^r = g^k$ 时，

$$G = \{e, g, \cdots, g^{m-1}\},$$

对任意 $1 \leqslant i < j \leqslant m$ 均有 $g^i \neq g^j$；

(2) 当对任意正整数 $r \neq k$ 均有 $g^r \neq g^k$ 时，

$$G = \{\cdots, g^{-1}, e, g, g^2, \cdots\}.$$ ▌

这个定理使我们对循环群的组成和运算一目了然，可以称为**循环群结构定理**.

例题 1 无限循环群 G 只有 2 个生成元.

证明 设 $G = \langle g \rangle$，那么 g 和 g^{-1} 均为 G 的生成元.

如果有 $n \in \mathbf{I}$ 使 g^n 亦为 G 的生成元，则必有 $m \in \mathbf{I}$ 使 $g = (g^n)^m = g^{mn}$. 而 G 为无限循环群，故 $g = g^{mn}$ 蕴涵 $mn = 1$，从而 $n = \pm 1$. ▌

命题 3 设 $G = \{e, g, \cdots, g^{m-1}\}$，正整数 p 与 m 互素且 $p < m$. 那么 $G = \langle g^p \rangle$.

证明 因为 $g^p \in \langle g \rangle$，故 $\langle g^p \rangle \subseteq \langle g \rangle$.

另一方面，p 与 m 互素．据第一章§6引理，必有整数 k,l 使

$$kp+ml=1.$$

于是

$$g=g^{kp}\cdot g^{ml}=(g^p)^k e=(g^p)^k\in\langle g^p\rangle.$$

所以，$\langle g\rangle=\langle g^p\rangle$． ▍

这个命题比较完整地回答了前面提出的循环群生成元的唯一性问题．

命题 4 无限循环群的每个子群都是循环群．

证明 设无限循环群 $G=\langle g\rangle$，H 是 G 的一个子群．e 为 G 之单位元．

如果 $H=\{e\}$，那么，H 自然是个循环群．

如果 $H\neq\{e\}$，那么，必有 $g^i\in H$，$i\in\mathbf{I}$，$i\neq 0$．假如 $i<0$，由 $g^i\in H$，H 为子群，可知 $g^{-i}\in H$，而 $0<-i$．所以，无论如何，可设有正整数 i，$g^i\in H$．在集合

$$\{i\in\mathbf{I}\mid g^i\in H,\ i>0\}$$

中取最小者，设为 m．

可以断言，对任意 $g^n\in H$ 都有 $m\mid n$．设

$$n=mq+r,\quad 0\leqslant r<m.$$

那么，由

$$g^n=(g^m)^q\cdot g^r,$$

可推出 $g^r=g^n\cdot(g^m)^{-q}\in H$，故必有 $r=0$，也就是 $m\mid n$．所以，

$$H=\langle g^m\rangle.$$ ▍

例题 2 设 $G=\langle g\rangle$是个无限循环群，$H=\langle g^i\rangle$和 $K=\langle g^j\rangle$是 G 的两个子群，$i,j\geqslant 0$．如果 d 是 i,j 的最高公因数，m 是 i,j 的最小公倍数，那么有

$$K\cap H=\langle g^m\rangle,\quad \langle K\cup H\rangle=\langle g^d\rangle.$$

证明 由于 m 是 i,j 的公倍数，必有 $a,b\in\mathbf{I}$ 使 $m=ai=bj$，故

$$g^m\in\langle g^i\rangle,\quad g^m\in\langle g^j\rangle.$$

因为$\langle g^m \rangle$是包含 g^m 的G 的子群的交集，自然应有

$$\langle g^m \rangle \in \langle g^i \rangle, \quad \langle g^m \rangle \subseteq \langle g^j \rangle;$$

进而$\langle g^m \rangle \subseteq \langle g^i \rangle \cap \langle g^j \rangle = K \cap H$.

反过来，若 G 的元素$g^t \in \langle g^i \rangle \cap \langle g^j \rangle$，则必有 $i \mid t$, $j \mid t$，即 t 是i, j 的一个公倍数. 而 m 是i, j 的最小公倍数，故 $m \mid t$,

$$g^t \in \langle g^m \rangle,$$

也就是 $H \cap K = \langle g^m \rangle$.

关于$\langle g^d \rangle = \langle H \cup K \rangle$. 因为 d 是i, j 的最高公因子，故有 $a, b \in \mathbf{I}$ 使得

$$ai + bj = d,$$

由于 g^{ia}, g^{jb}均在$H \cup K$ 生成的子群$\langle H \cup K \rangle$中，故

$$g^d = g^{ia} g^{jb} \in \langle H \cup K \rangle.$$

从而 g^d 生成的子群包含在$\langle H \cup K \rangle$中.

另一方面，在§2 中，我们已经分析过，由只含两个元素 a, b 的集合S 所生成的子群中，每个元素必形如

$$a^t b^s \cdots a^p b^q, \quad t, s, \cdots, p, q \in \mathbf{I}.$$

在这里，$a = g^i$, $b = g^j$. 所以，$\langle \{g^i, g^j\} \rangle$的元素必形如

$$g^{it} g^{js} \cdots g^{ip} g^{iq} = g^{ui+vj}, \quad u, v \in \mathbf{I}.$$

由于 $d \mid i$, $d \mid j$，故 $g^{ui+vj} \in \langle g^d \rangle$. 所以

$$\langle H \cup K \rangle = \langle \{g^i, g^j\} \rangle = \langle g^d \rangle. \qquad \blacksquare$$

无限循环群的最典型代表是整数加法群(I, +). 整数 1 是它的一个生成元，每个正整数 i 等于i 个 1 相加，每个负整数 j 等于 $-j$ 个 -1 相加.

上述几个命题套在(I, +)上，即是说，它的每个子群恰好由某个非负整数 n 生成；两个非负整数 i, j 的最高公因数为d，最小公倍数为 m，则

$$\langle i \rangle \cap \langle j \rangle = \langle d \rangle, \quad \langle \{i, j\} \rangle = \langle \langle i \rangle \cup \langle j \rangle \rangle = \langle m \rangle.$$

关于有限循环群，可用下述方法得到一个典型代表.

在整数集 I 中，用第一章§3 例 12 的方法得一商集

$$\mathbf{I}_{\sim n}=\{[0],[1],\cdots,[n-1]\},$$

其中

$$[0]=\{\cdots,-n,0,n,\cdots\},$$
$$[1]=\{\cdots,-n+1,1,n+1,\cdots\},$$
$$\cdots,$$
$$[n-1]=\{\cdots,-1,n-1,2n-1,\cdots\}.$$

要特别注意的是,等价类的代表元素是可以任意取的,例如 $[0]=[n]=[-4n]$. 在写集合 $\mathbf{I}_{\sim n}$ 的元素时,只要取 $\mathbf{I}$ 对等价关系 $\sim$ 的一个完全集作代表. 现在取的 $\{0,1,\cdots,n-1\}$ 即为一完全集.

为书写方便,记 $\mathbf{I}_{\sim n}$ 为 $\bar{\mathbf{I}}$.

下面打算用一个自然的方法在 $\bar{\mathbf{I}}$ 中定义一个运算,并使 $\bar{\mathbf{I}}$ 在此运算之下作成群.

规定,$\bar{\mathbf{I}}$ 的任意元素 $[a]$,$[b]$ 对应 $\bar{\mathbf{I}}$ 中元素 $[a+b]$,即 $[a]$,$[b]$ 对应 $a+b$ 所在的等价类.

例如,当 $n=5$ 时,等价类 $[3]$,$[4]$ 对应等价类

$$[3+4]=\{\cdots,-3,2,7,\cdots\}.$$

同样,等价类

$$[-9]=\{\cdots,-9,-4,1,\cdots\} \tag{1}$$

和等价类

$$[7]=\{\cdots,-3,2,7,\cdots\} \tag{2}$$

对应等价类

$$[-9+7]=\{\cdots,-2,3,8,\cdots\}.$$

这种对应方式乃是把两个等价类取定后,并不限于必须用某一完全集中的元素作代表,而是任取两个元素作代表,于是可把它们记为 $[a]$,$[b]$. 然后,即用任取的代表元 a 和 b 来确定等价类 $[a]$,$[b]$ 所对应的等价类.

然而,这里发生了一个严重问题,这真的是个对应吗? 也就是问,这真的是个 $\bar{\mathbf{I}}\times\bar{\mathbf{I}}$ 到 $\bar{\mathbf{I}}$ 的映射吗? 又等于问,按着这种方式 $[a]$,$[b]$ 对应的是 $\bar{\mathbf{I}}$ 的一个"确定的"元素吗?

具体说来，等价类(1)和等价类(2)既可以用 -9 和 7 分别代表之，也可以用 1 和 47 分别代表之. 按前一种代表方式，它们应对应 $[-9+7]$，而用后一种代表方式，它们又应对应 $[1+47]$. 那么，能保证

$$[-9+7]=[1+47]$$

成立吗？我们有

命题 5 在 $\bar{I}$ 中，如果 $[a_1]=[a_2]$，$[b_1]=[b_2]$，则

$$[a_1+b_1]=[a_2+b_2].$$

证明 如果 $[a_1]=[a_2]$，即 $a_1\sim a_2$，也就是 $n\mid(a_1-a_2)$. 即必有整数 u 使

$$a_1=a_2+un.$$

同样，$[b_1]=[b_2]$ 导致有 $v\in I$ 使

$$b_1=b_2+vn.$$

加起来，得

$$a_1+b_1=(a_2+b_2)+(u+v)n,$$

也就是 $(a_1+b_1)-(a_2+b_2)$ 可以被 n 整除，

$$a_1+b_1\sim a_2+b_2,$$

从而 $[a_1+b_1]=[a_2+b_2]$. ▌

这个命题解决了所给运算定义的合理性，按这样的规定，$[a],[b]\in\bar{I}$ 对应 $\bar{I}$ 的一个确定的元素 $[a+b]$. 我们把这种运算称为商集 $\bar{I}$ 的加法，记为$\boxplus$，从而有，

$$[a]\boxplus[b]=[a+b].$$

命题 6 $(\bar{I},\boxplus)$ 是个交换群.

证明 对任意 $[a],[b],[c]\in\bar{I}$，

$([a]\boxplus[b])\boxplus[c]$

$=[a+b]\boxplus[c]$ （$\boxplus$的定义）

$=[(a+b)+c]$ （$\boxplus$的定义）

$=[a+(b+c)]$ （整数加法可结合）

$=[a]\boxplus[b+c]$ （$\boxplus$的定义）

$=[a]\boxplus([b]\boxplus[c])$ （$\boxplus$的定义）.

即$(\bar{I},\boxplus)$满足结合律.

对任意$[a]\in\bar{I}$,由于数0的性质,有

$$[0]\boxplus[a]=[0+a]=[a],$$
$$[a]\boxplus[0]=[a+0]=[a].$$

即$[0]$是恒等元.

对任意$[a]\in\bar{I}$,取等价类$[-a]$,有

$$[a]\boxplus[-a]=[a+(-a)]=[0],$$
$$[-a]\boxplus[a]=[(-a)+a]=[0].$$

即$[-a]$是$[a]$的逆元素.

由于整数加法群满足交换律,故对任意$[a],[b]\in\bar{I}$,恒有

$$[a]\boxplus[b]=[a+b]=[b]\boxplus[a].$$

从而$(\bar{I},\boxplus)$是个交换群. ▌

群$(\bar{I},\boxplus)$含n个元素,对任意正整数m, $1\leqslant m<n$, $[m]=m[1]$.这说明群$(\bar{I},\boxplus)$是由$[1]$生成的循环群.

这种用等价类作元素构造出来的运算系统在《抽象代数》中将占极重要位置,请读者趁本节内容简单、负担轻的机会把这个群的定义仔细玩味玩味.

与命题4中的无限循环群相对照,可以讨论有限循环群的子群.

例题3 有限循环群$G=\{e,g,\cdots,g^{n-1}\}$的每个子群H都是循环群.

证明 设

$$H=\{e,g^i,g^j,\cdots,g^k\},$$

其中$i,j,\cdots,k$是大于0小于n的整数,且两两不同.设l是它们之中的最小者.

可以断言,l必能整除$i,j,\cdots,k$.设

$$i=ql+r,\quad 0\leqslant r<l.$$

由于 $g^i\in H$, $g^l\in H$,从而

$$g^r=g^i((g^l)^q)^{-1}\in H.$$

由 l 之最小性推知 $r=0$.所以,

$$i=lq,\quad j=lp,\quad \cdots,\quad k=lm,$$

$$H=\{e,(g^l)^q,(g^l)^p,\cdots,(g^l)^m\}\subseteq\langle g^l\rangle.$$

另一方面,$g^l\in H$, $\langle g^l\rangle\subseteq H$,故 $H=\langle g^l\rangle$. ∎

例题 4 在 n 次循环群

$$G=\{e,g,\cdots,g^{n-1}\}$$

中,若 n 能分解为正整数 s,t 之积,即 $n=st$,则 G 有而且只有一个子群含 t 个元素.

证明 我们看 g^s 生成的子群$\langle g^s\rangle$.形式上它含有

$$e,g^s,g^{2s},\cdots,g^{ts},\cdots,$$

但 $g^{ts}=g^n=e$, $g^{(t+1)s}=g^{n+s}=g^ng^s=eg^s=g^s$, $\cdots$,所以,从$(g^s)^t$起,后面的元素就与前列元素重复了.$\langle g^s\rangle$不重复的元素最多可能是

$$e,g^s,(g^s)^2,\cdots,(g^s)^{t-1}. \qquad (*)$$

现在来说明上述 t 个元素必然两两不同,这是因为,G 的 n 元循环群

$$e,g,\cdots,g^s,g^{s+1},\cdots,g^{n-1}$$

两两不同,(*)乃是其中的一部分而已.

这就解决了本题的存在性证明,下面来解决唯一性问题.

设 G 中还有一个元素 g^r,它生成的子群也恰好含 t 个元素,我们要证明$\langle g^r\rangle=\langle g^s\rangle$.这里要注意,只要证明两群相等,不是去证明 $g^r=g^s$,那可能是办不到的.

事实上,群$\langle g^r\rangle$的 t 个元素

$$e,g^r,g^{2r},\cdots,g^{(t-1)r}$$

两两不同,且 $g^{tr}\in\langle g^r\rangle$,必知 $g^{tr}=e$.再用命题 1,必有 $n\mid(tr)$.设 $tr=kn=k(st)$,则得

$$r=ks.$$

于是有 $g^t \in \langle g^s \rangle$，进而 $\langle g^t \rangle \subseteq \langle g^s \rangle$.

另一方面，已经知道 $\langle g^t \rangle$ 本身就含 t 个元素，而 $\langle g^s \rangle$ 也是含 t 个元素，故 $\langle g^s \rangle = \langle g^t \rangle$ ∎

例如，6 阶循环群

$$\{e, a, a^2, a^3, a^4, a^5\}$$

只有一个三元子群

$$H = \{e, a^2, a^4\}.$$

这个子群是 a^2 生成的，也是 a^4 生成的，即

$$H = \langle a^2 \rangle = \langle a^4 \rangle.$$

习 题 四

1. 给出循环群 $(I_{\sim\infty}, \boxplus)$ 的所有子群，且指出每个子群的生成元（它的每个子群都是循环群，由一个元素生成）.

2. 在循环群 $(I_{\sim 24}, \boxplus)$ 中，把子集

$$\{[4], [6], [8]\}$$

生成的子群写出来，它可由哪些单个元素生成之，把该子群按生成元升幂排列其元素.

3. 证明：

$$\{1, -1, i, -i\}, \left\{1, -\frac{1}{2} + i\frac{\sqrt{3}}{2}, -\frac{1}{2} - i\frac{\sqrt{3}}{2}\right\}$$

在数的乘法之下是个循环群，其中 i 是纯虚数.

4. 群 G 有 4 个元素 e, a, b, c，已经知道 G 不是循环群，请完成乘法表

	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

§5 阶 数

定义 1 群 G 中元素的个数称为 G 的**阶数**. 当 G 有无穷多个

元素时，说 G 是**无限阶的**；当 G 的元素个数有限时，用 $|G|$ 代表 G 的元素的个数.

对于群 G 的元素 a，如果有非负整数 n，使得 $a^n=e$，且 n 为使上等式成立的最小的非负整数，则说 a 是有限阶的，**阶数**为 n. 如果找不到这样的数，则说 a 是无限阶的. 也有人把元素的阶数称为元素的**周期**.

这一节，我们要讨论群中元素的阶数与群的阶数的关系，群的阶数与其诸子群阶数的关系，得到有名的又有用的拉格朗日定理.

为了处理这个问题，需要引进群 G 对其子群 H 的陪集概念，而陪集从此以后就不断地出现在群的各种问题的讨论中，是本课程的最重要的概念之一. 同时，对初学者来说也是一个不太容易理解的概念之一.

希望读者在一开始接触"陪集"时，能多分析一些实例而不是硬记抽象定义.

例 1 在 S_3 中，$(1\ 2\ 3)$的阶数等于 3.

例 2 在$(\mathbf{I},+)$中，任意非零整数 m 的阶是无限的.

例 3 设 G 为从 $\mathbf{I}$ 到 $\{1,-1\}$ 的所有映射作成的集合. 对每对映射 $f,g\in G$，令它们对应 G 中元素 h（也就是 $\mathbf{I}$ 到 $\{1,-1\}$ 的映射），

$$h(j)=f(j)\cdot g(j),\quad j\in\mathbf{I}.$$

也就是说，让 f,g 对应这样一个从 $\mathbf{I}$ 到 $\{1,-1\}$ 的映射 h，它把整数 j 变成数 $f(j)$ 和数 $g(j)$ 的乘积. 由于 $f(j),g(j)$ 均或为 1 或为 -1，故它们的乘积也是 1 或 -1.

这样，我们得到一个 $G\times G$ 到 G 的映射，称为 G 上**函数乘法**，记为 $h=f\times g$.

G 中元素 i，它把所有整数都变成 1，即

$$i(j)=1,\quad 任意\ j\in\mathbf{I},$$

是$(G,\times)$的一个恒等元. 对任意 $f\in G$，从 $\mathbf{I}$ 到 $\{1,-1\}$ 的映射

$$g(j)=-f(j),\quad j\in\mathbf{I}$$

是 f 的一个逆元素.

G 中三元素 f_1,f_2,f_3 在函数乘法之下的可结合性可归纳结为在任何整数 j 处,数 $f_1(j)$,$f_2(j)$ 和 $f_3(j)$ 乘法的可结合性,故 $(G,\times)$ 满足结合律.

这就验证了 $(G,\times)$ 是一个群.而且,它是个无限群.例如,令 g_k 代表把 $k\in\mathbf{I}$ 变成 1,而将其余整数均变为 -1 的函数,则 g_1, g_2,…就是不同的映射.

同时,对于每个 $f\in G$,我们有

$$(f\times f)(j)=f(j)\cdot f(j)=1,\quad j\in\mathbf{I}.$$

也就是 $f\times f=i$,i 为恒等元.

这说明,G 中非单位元之阶数均为 2.

这个例于告诉我们,G 之每个元素之阶数均有限并不意味着 G 本身的阶数有限.

命题 1 设 a 是群 G 的一个元素.那么 a 的阶数与子群 $\langle a\rangle$ 的阶数相等.

证明 首先,我们要说明,元素 a 是有限阶的,当而且仅当,有整数 t 使得 $a^t=e$.

因为,若 $\mathbf{I}$ 的子集

$$A=\{m\in\mathbf{I}\mid a^m=e\}$$

非空($t\in A$),则一定含非负整数(若 $t<0$,则 $-t\in A$).根据整数集的性质,A 中必有最小的非负整数 n 存在.从而 a 的阶数有限,就是 n.

进而,还可以说明,元素 a 是有限阶的,当而且仅当,有不相同的整数 r,s 使 $a^r=a^s$.

这是因为,若 a 阶数有限,为 m,那么必有

$$a^m=a^0.$$

反过来,$r\neq s$ 但 $a^r=a^s$.则使得 $a^{r-s}=e$.据上面分析,a 阶数必有限.

据§4 命题 1 知,元素 a 的阶数有限时,$\langle a\rangle$ 有限,且当 a 的

阶数为 m 时，$\langle a\rangle$恰为

$$\{e, a, \cdots, a^{m-1}\};$$

从而$\langle a\rangle$的阶数亦为 m.

如果 a 是无限阶的，那么，对任意不同的整数 r, k 必有 $a^r \neq a^k$. 于是，据 § 4 命题 2，群$\langle g\rangle$的阶数也是无限的. ▌

定义 2 设 H 是群 G 的一个子群，H 在群 G 中确定关系 ~ 如下，$a, b \in G$，$a \sim b$ 当而且仅当 $ab^{-1} \in H$，称 ~ 是 H 在 G 中确定的右关系.

命题 2 设 H 是 G 的子群，则 H 在 G 上确定的右关系 ~ 是个等价关系.

证明 对任意 $a \in G$，因为 $aa^{-1} = e \in H$，故 $a \sim a$，这说明 ~ 有反身性.

如果 $a, b \in G$，$a \sim b$，即 $ab^{-1} \in H$，由于 H 是子群，故有

$$(ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1} \in H,$$

$b \sim a$，这说明 ~ 具有对称性.

如果 $a, b, c \in G$，$a \sim b$，$b \sim c$，即

$$ab^{-1} \in H,\ bc^{-1} \in H,$$

由于 H 是 G 的子群，就必有

$$(ab^{-1})(bc^{-1}) = a(b^{-1}b)c^{-1} = ac^{-1} \in H,$$

也就是 $a \sim c$，说明 ~ 有传递性.

所以，~ 是 G 上的一个等价关系. ▌

例 4 在群$(\mathbf{I}, +)$中，取 $H = \langle 7\rangle$，对任意 $i, j \in \mathbf{I}$，$i \sim j$ 当而且仅当 $i - j \in \langle 7\rangle$，当而且仅当 $7 \mid (i - j)$.

例 5 在 3 阶对称群 $\mathbf{S}_3$ 中，取

$$H = \{i_{s_3}, (1\ 2)\},$$

看由它划分的等价关系：

$$\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix} = (1\ 2),$$

知道

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\sim\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}^{-1}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=(2\ 3).$$

同理

$$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\sim\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=(1\ 3).$$

我们可以看出，对于群 G 的一个子群 H，还可定义另一个等价关系，对任意 $a,b\in G$，$a\simeq b$，当而且仅当 $b^{-1}a\in H$，称为**左关系**.

一般来说，H 所确定的右关系 $\sim$ 和左关系 $\simeq$ 并不一定相同. 比如，例 5 中

$$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=(1\ 3)\notin H,$$

即知 $(2\ 3)\sim(1\ 2\ 3)$；而对于 $\simeq$，$(2\ 3)$ 与循环 $(1\ 2\ 3)$ 不等价.

定义 3 对群 G 之任意非空子集 A,B，称 G 的子集

$$\{g\in G\mid g=ab,\ a\in A,\ b\in B\}$$

为 A 与 B 的**乘积**，记为 AB.

当 A 为子群，$B=\{b\}$ 时，记 $Ab=AB$，并称 Ab 是 A 在 G 中的一个**右陪集**.

$A=\{a\}$，B 为子群，则记 $aB=AB$，并称 aB 为 B 在 G 中的一个**左陪集**.

例 6 条件如例 5，则

$$\begin{aligned}H(1\ 2\ 3)&=\{i_{S_3}(1\ 2\ 3),(1\ 2)(1\ 2\ 3)\}\\&=\{(1\ 2\ 3),(2\ 3)\},\\H(1\ 3\ 2)&=\{i_{S_3}(1\ 3\ 2),(1\ 2)(1\ 3\ 2)\}\\&=\{(1\ 3\ 2),(1\ 3)\}.\\H(2\ 3)&=\{i_{S_3}(2\ 3),(1\ 2)(2\ 3)\}\\&=\{(2\ 3),(1\ 2\ 3)\},\end{aligned}$$

$$H(1\ 3)=\{i_{S_3}(1\ 3),(1\ 2)(1\ 3)\}$$
$$=\{(1\ 3),(1\ 3\ 2)\},$$
$$(1\ 2\ 3)H=\{(1\ 2\ 3)i_{S_3},(1\ 2\ 3)(1\ 2)\}$$
$$=\{(1\ 2\ 3),(1\ 3)\},$$
$$(1\ 2)H=\{(1\ 2)i_{S_3},(1\ 2)(1\ 2)\}$$
$$=\{i_{S_3},(1\ 2)\},$$
$$(1\ 3\ 2)H=\{(1\ 3\ 2)i_{S_3},(1\ 3\ 2)(1\ 2)\}$$
$$=\{(1\ 3\ 2),(2\ 3)\}.$$

例题 1 如果 H 是 G 的子群,则 $HH=H$.

证明 对任意 $g\in HH$,由 HH 的定义,必有 $h,k\in H$, $g=kk$.而 H 是子群,故 $hk\in H$;也就是 $g\in H$,即 $HH\subseteq H$.

另一方面,任意 $g\in H$ 都可写成

$$g=ge,\ g\in H,\ e\in H.$$

从而,$g\in HH$,即 $H\subseteq HH$.

总结之,得 $HH=H$. ▌

命题 3 设 H 是 G 的子群,$\sim$是 H 在 G 中确定的右关系,那么元素 $a\in G$ 在等价关系$\sim$之下的等价类恰好是 H 的右陪集 Ha.

证明 按等价类的定义(见第一章§3),元素 a 的等价类是 G 的子集

$$S_a=\{b\in G\mid b\sim a\}.$$

现在来证明 $S_a=Ha$.

如果 $b\in S_a$,即 $b\sim a$, $ba^{-1}\in H$.令 $h=ba^{-1}$,则 $b=ha\in Ha$,这说明

$$S_a\subseteq Ha.$$

反之,如果 $b\in Ha$, $b=ha$, $h\in H$. 那么, $ba^{-1}=h\in H$, $b\sim a$.从而 $b\in S_a$.这说明 $Ha\subseteq S_a$.进而,有 $Ha=S_a$. ▌

推论 设 H 是群 G 的子群,$a,b\in G$.那么 $ab^{-1}\in H$ 当而且仅当 $Ha=Hb$.

事实上,$ab^{-1}\in H$,即 $a\sim b$.而 $a\sim b$ 的充要条件是它们的等价类相等,即 $Ha=Hb$. ▌

命题 4 如果 H 是群 G 的有限子集,则子集 Ha 的元素个数等于 H 的阶数.

证明 在有限集合 H 和 Ha 之间建立一个双射即可.

定义 H 到 Ha 的一个映射 f:

$$f(h)=ha,\quad h\in H.$$

对任意 $g\in Ha$,必有 $h_1\in H$ 使 $g=h_1a$.从而 $f(h_1)=h_1a=g$, $g\in \mathrm{Img}\, f$, g 为满射.

如果有 $h_2,h_3\in H$ 使得 $f(h_2)=f(h_3)$,即

$$f(h_2)=h_2a=h_3a=f(h_3),$$

由于群中有消去律,就应有 $h_2=h_3$,这说明 f 是单射.

所以,H 和 Ha 元素个数相同. ▌

拉格朗日(Lagrange)定理 设 G 是个有限群.那么 G 的任意子群 H 的阶数一定整除 G 的阶数,即 $|H|\,|\,|G|$.

证明 由第一章§3 知道,G 的一个等价关系决定它的一个分类.

关于子群 H 的右陪集恰为等价关系 $\sim$ 的等价类.所以,两个陪集或不交或相同.又因为 G 是有限的,它只含有限个 H 的右陪集.我们可取 $a_1,a_2,\cdots,a_k$ 为等价关系 $\sim$ 之下的一个完全集,则

$$G=Ha_1\cup Ha_2\cup\cdots\cup Ha_k$$

是两两不交的等价类的并集,即得 G 的一个分类.

因此,G 的元素被分成 k 组,每个元素在而且只在其中一组.同时,每组元素的个数都是 $|H|$(命题 4),所以 $|G|=k|H|$. ▌

推论 1 设 G 是个有限群.那么,它的任意元素 a 的阶数都能整除 G 的阶数.

事实上,由命题1知元素 a 的阶数与子群 $\langle a\rangle$ 的阶数相等;由拉格朗日定理知 $\langle a\rangle$ 的阶数整除 G 的阶数;从而 a 的阶数整除 $|G|$. ▌

推论2 设 G 是个有限群,$|G|$ 是个素数.那么 G 只有 $\{e\}$ 和 G 两个子群.

这是因为素数只有1和自己两个因子. ▌

推论3 设 G 是个有限群,$|G|$ 是个素数.那么 G 必为循环群.

事实上,取 G 之元素 $a\neq e$,则 a 的阶数不等于1,$\langle a\rangle$ 的阶数要整除 $|G|$,故有

$$|\langle a\rangle|=|G|.$$

一个有限集的子集和该集合元数相等,则该子集必与此集合相等,于是有 $\langle a\rangle=G$. G 是由 a 生成的循环群. ▌

例题2 设 G 是有限群,H 是其子群,而且 $|G|=2|H|$.那么,如果 $a,b\in G$ 但 $a\notin H$, $b\notin H$,则必有 $ab\in H$.

证明 当 $|G|=2|H|$ 时,G 只有 H 的两个陪集,一个是 H.

对于 G 的任意元 a,如果 $a\notin H$,则陪集 Ha 与 H 不相交,故必有 $G=H\cup Ha$.

进而,如果 $a,b\notin H$,则 $b^{-1}\notin H$.从而 a,b 在同一个陪集内,a,b^{-1} 也在同一个陪集内.换言之,$a\sim b^{-1}$.于是,

$$a(b^{-1})^{-1}=ab\in H.$$ ▌

例题3 设 G 是有限群,H 是其子群,而且 $|G|=2|H|$.那么 H 在 G 中的左陪集也是右陪集.

事实上,此时 H 只有两个左陪集,一个是 H,另一个是 aH,$a\notin H$.且 $G=H\cup aH$.

同理,G 只有两个右陪集,只要 $a\notin H$,则必有 $G=H\cup Ha$.综合之,即知 $Ha=aH$. ▌

例题4 对称群 $\mathbf{S}_4$ 中,子群

$$H=\langle\{(1\ 2\ 3),(1\ 2)(3\ 4)\}\rangle$$

阶数为 12,但 H 不含阶数为 6 的子群.

证明 令 $a=(1\ 2\ 3)$, $b=(1\ 2)(3\ 4)$. 计算得 H 的元素

$$
\begin{aligned}
a&=(1\ 2\ 3), & a^2&=(1\ 3\ 2),\\
ba&=(2\ 4\ 3), & (ba)^2&=(2\ 3\ 4),\\
ab&=(1\ 3\ 4), & (ab)^2&=(1\ 4\ 3),\\
b&=(1\ 2)(3\ 4), & bab&=(1\ 4\ 2).
\end{aligned}
$$

由于 H 的阶数是 S_4 阶数的因子, $|H|\,|\,24$. 上面已经知道 9 个不同元素(包括恒等置换),故 H 的阶数为 12 或者 24.

由于 a,b 都是偶置换, H 的每个元素都是若干个 a,b 之积,从而 H 的元素只能是偶置换. 所以, $H\neq S_4$, $|H|=12$.

设 K 是 H 的子群,且 $|K|=6$. 我们已经看到 H 中至少有 t 个元素是 3 循环. 于是, K 至少不含一个 3 循环 c, $c\notin K$.

但是,前面例题已指明,当 $|H|=2|K|$ 时, $c\notin K$,则必有 $c^2\in K$. 而 $c^3=e$,也就是, $c^2=c^{-1}\in K$,这与 $c\notin K$ 矛盾. ▎

这个例题表明,由拉格朗日定理,不能得出这样的结论:群 G 的阶数为 n,则对 n 的每个因数 d, G 必有 d 阶子群.

但,当 G 为循环群时,我们已经有 §4 之例题 4.

例题 5 设 a,b 是交换群 G 的元素,它们的阶数分别为 m, n. 如果 m 和 n 互素,那么 ab 的阶数为 mn.

证明 一方面

$$(ab)^{mn}=a^{mn}b^{mn}=(a^m)^n(b^n)^m=e.$$

另一方面,对任意 $t\in \mathbf{I}$,如果 $(ab)^t=e$,那么,

$$e=(ab)^{tn}=a^{tn}(b^n)^t=a^{tn}.$$

而 a 的指数为 m,从而 $m\,|\,(tn)$. 同理, $n\,|\,(tm)$.

但是 m,n 互素,故 $m\,|\,t$, $n\,|\,t$. 进而 $(mn)\,|\,t$.

所以, ab 的阶数刚好是 mn. ▎

命题 5 设 G 是个有限交换群. 如果 $a\in G$ 的阶数 t 大于等于 G 中所有元素的阶数,那么每个元素的阶数均可整除 t.

证明　任取 $b\in G$，设 b 的阶数为 s. 将 t 和 s 写成素因子之连乘积，设

$$t=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n},\quad 0\leqslant\alpha_i\in\mathbf{I},$$
$$s=p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n},\quad 0\leqslant\beta_j\in\mathbf{I}.$$

如果 s 不能整除 t，那么必有某个 $\beta_j>\alpha_j$. 为方便计，设 $\alpha_1<\beta_1$，即有

$$t=p^{\alpha}t_1,\quad (p,t_1)=1,$$
$$s=p^{\beta}s_1,\quad (p,s_1)=1.$$

于是，b^{s_1} 的阶数为 p^{β}，而 $a^{p^{\alpha}}$ 的阶数为 t_1，并且 p^{β} 和 t_1 也是互素的，据上面例题，立知 G 的元素 $a^{p^{\alpha}}b^{s_1}$ 的阶数为 $p^{\beta}t_1>t$，得一矛盾. ▌

例题 6　$\mathbf{I}_{11}$ 的非零元构成的乘法群是不是循环群？

证明　$\mathbf{I}_{11}-\{0\}$ 是个 10 元群. 计算 2^* 的各次幂，得

$$2^*,4^*,8^*,5^*,10^*.$$

到这时，我们不必算下去了，因为 2^* 的阶数要整除 $\mathbf{I}_{11}-\{0\}$ 的阶数 10，从而只能是

$$1,2,5,10.$$

到此为止，2^* 的 5 个不同方幂中尚未出现恒等元 1^*，所以 2^* 的阶数一定是 10. 从而

$$\mathbf{I}_{11}-\{0\}=\langle 2^*\rangle.$$ ▌

例题 7　设群 G 满足条件

$$a^2b^2=b^2a^2,\quad 对任意\ a,b\in G.$$

证明：G 之所有周期为奇数的元素和恒等元 e 的集合 H 是 G 的一个子群，且 H 是个交换群.

证明　若 $a,b\in H$，有非负整数 m,n，

$$a^{2m+1}=e,\quad b^{2n+1}=e,$$

那么

$$ab = a^{2m+2}b^{2n+2} = a^{2m}a^2b^2b^{2n} = a^{2m}b^2a^2b^{2n}$$
$$= b^2a^{2m+2}b^{2n} = \cdots = b^{2n+2}a^{2m+2} = ba;$$

也就是说 H 中任意两个元素乘积可换(现在还没证明 $ab \in H$).

对上面的 $a, b \in H$,由于它们乘积可换,故

$$(ab)^{(2m+1)(2n+1)} = a^{(2m+1)(2n+1)}b^{(2n+1)(2m+1)} = e.$$

从而元素 ab 的周期应当整除$(2m+1)(2n+1)$;也就是说,ab 的周期必为奇数,$ab \in H$.

由于 a 和 a^{-1} 恒有相同周期,当 $a \in H$ 时必有 $a^{-1} \in H$.

所以,H 是个交换群 ∎

习 题 五

1. 设 G 是个群,$a, b \in G$. 证明:ab 的阶数与 ba 的阶数总是相同的.

2. 若群 G 只含唯一的一个 2 阶元素 a,那么对任意 $x \in G$ 恒有 $ax = xa$.

3. 设 G 是个交换群,则 $H = \{g \in G \mid g$ 阶数有限$\}$是 G 的一个子群.

4. 若 4 元群 G 中任何元素之阶数均不为 4,则 G 是个交换群.

5. G 的阶数是 p^2,p 是个素数. 若 G 不是循环群,则对任意 $g \in G$ 恒有

$$g^p = e.$$

6. 设 G 是个群,H 是 G 的所有非平凡子群的交集. 如果 $H \neq \{e\}$,那么 H 的每个元素的阶数都是有限的.

7. 在非零复数作成的乘法群中,求复数 $\alpha = \frac{1}{2} + \mathrm{i}\frac{\sqrt{3}}{2}$的周期.

§6* 群的外直积

设(G, Δ)是个群,$(H, \circ)$也是个群. 作为集合,我们可以考虑集合 G 和集合H 的笛卡尔积$G \times H$.

那么,是否可以利用群(G, Δ)的原有运算 Δ 和群$(H, \circ)$的原有运算$\circ$而得到集合 $G \times H$ 的一个运算呢? 进一步,还希望

$G\times H$ 在新得到的运算之下构成群.

这种想法是极其自然的.例如,平面解析几何学中,就是把实数的加法、乘法用到平面 $\mathbf{R}\times\mathbf{R}$ 上,得到平面上向量的加法以及数乘运算的.

线性代数学中,讨论线性空间的直和、欧氏空间的直和,为矩阵或变换化成各式各样的标准形式提供了有力工具.

本课程把关于群的直积方法的学习分成两部分.一部分放在本节.另一部分,用同构的观点研究直积与子群的关系,放到第三章.

这一节内容比较简单,但涉及到的概念和符号较多,读者最好能用自己的思路处理有关证明部分,然后再对照书上所给证明加以检查.

现在,设 (G,Δ) 是个群,$(H,\circ)$ 也是个群.在 G 和 H 的笛卡尔积 $G\times H$ 上,规定一个二元运算如下:

对任意 $(a,x),(b,y)\in G\times H$,令其对应 $G\times H$ 中的元素

$$(a\Delta b,x\circ y).$$

由于 Δ 是 G 上二元运算,$\circ$ 是 H 上二元运算,$a\Delta b$ 确实是 G 的元素,$x\circ y$ 确实是 H 的元素,从面 $(a\Delta b,x\circ y)$ 确实是 $G\times H$ 的元素

这样,就得到一个 $(G\times H)\times(G\times H)$ 到 $G\times H$ 的映射,也就是 $G\times H$ 上的二元运算,记为 $\otimes$,即

$$(a,x)\otimes(b,y)=(a\Delta b,x\circ y).$$

命题 1 在如上的规定之下,$(G\times H,\otimes)$ 作成一个群.

证明 对任意 $(a,x),(b,y),(c,z)\in G\times H$,有

$$\begin{aligned}
&[(a,x)\otimes(b,y)]\otimes(c,z)\\
&=(a\Delta b,x\circ y)\otimes(c,z) &&(\otimes\text{的定义})\\
&=((a\Delta b)\Delta c,(x\circ y)\circ z) &&(\otimes\text{的定义})\\
&=(a\Delta(b\Delta c),x\circ(y\circ z)) &&(\Delta\text{ 和}\circ\text{的结合律})\\
&=(a,x)\otimes(b\Delta c,y\circ z) &&(\otimes\text{的定义})
\end{aligned}$$

$$=(a,x)\otimes[(b,y)\otimes(c,z)]. \quad (\otimes\text{的定义})$$

这说明$\otimes$满足结合律.

设 e_G 是群(G,Δ)的恒等元,e_H 是$(H,\circ)$的恒等元.那么,对任意$(a,x)\in G\times H$,有

$$\begin{aligned}&(e_G,e_H)\otimes(a,x)\\&=(e_G\Delta a,e_H\circ x) &&(\otimes\text{的定义})\\&=(a,x). &&(e_G,e_H\text{ 的性质})\end{aligned}$$

这说明(e_G,e_H)是 $G\times H$ 的左恒等元.

对任意$(a,x)\in G\times H$,即 $a\in G$, $x\in H$,由于 G 和 H 都是群,a 在 G 中有逆 a^{-1}, x 在 H 中有逆元 x^{-1} 使得

$$a^{-1}\Delta a=e_G, \quad x^{-1}\circ x=e_H,$$

从而$(a^{-1},x^{-1})\in G\times H$ 且使得

$$\begin{aligned}&(a^{-1},x^{-1})\otimes(a,x)\\&=(a^{-1}\Delta a,x^{-1}\circ x) &&(\otimes\text{的定义})\\&=(e_G,e_H) &&(a^{-1},x^{-1}\text{的性质})\end{aligned}$$

这说明 $G\times H$ 在$\otimes$运算之下每个元素都有左逆元.

据本章§1,知$(G\times H,\otimes)$是个群. ▌

同样,对任意 n 个群$(G_i,\circ_i)$, $i=1,2,\cdots,n$.我们可在笛卡尔积 $G_1\times\cdots\times G_n$ 上规定,任意$(a_1,a_2,\cdots,a_n),(b_1,b_2,\cdots,b_n)\in G_1\times\cdots\times G_n$ 对应

$$(a_1\circ_1 b_1,a_2\circ_2 b_2,\cdots,a_n\circ_n b_n),$$

则得到 $G_1\times\cdots\times G_n$ 上的一个运算,记为$\otimes$,即

$$(a_1,\cdots,a_n)\otimes(b_1,\cdots,b_n)=(a_1\circ_1 b_1,\cdots,a_n\circ_n b_n),$$

这样,$(G_1\times\cdots\times G_n,\otimes)$是个群.

例 1 取 $G_1=G_2=\cdots=G_n=\mathbf{R}$,诸运算$\circ_i$ 都是实数加法,则

$$(r_1,r_2,\cdots,r_n)\otimes(s_1,s_2,\cdots,s_n)=(r_1+s_1,\cdots,r_n+s_n)$$

就是大家熟知的实的 n 维线性空间中向量的加法.

例 2 设 G 是所有 n 阶可逆矩阵在矩阵乘法$\times_n$ 之下构成的

群，H 是所有 m 阶可逆矩阵在矩阵乘法 $\times_m$ 之下构成的群.

对任意 $A,B\in G$，$X,Y\in H$，也就是

$$(A,X)\in G\times H,\quad (B,Y)\in G\times H.$$

规定

$$(A,X)\otimes(B,Y)=(A\times_n B, X\times_m Y),$$

则 $G\times H$ 在$\otimes$之下构成群.

下一章里，我们会看到$(G\times H,\otimes)$与所有形如

$$\begin{pmatrix} A & 0 \\ 0 & X \end{pmatrix}\begin{matrix} m\text{ 行} \\ n\text{ 行} \end{matrix}$$

$$\quad m\text{ 列}\qquad n\text{ 列}$$

的可逆分块矩阵在矩阵乘法之下构成的矩阵的代数结构是相同的.

读者自己可以证明，群(G,Δ)和群$(H,\circ)$用前述方法引出的群$(G\times H,\otimes)$是交换的，当而且仅当群(G,Δ)和群$(H,\circ)$都是交换的.

定义 设$(G_1,\circ_1),\cdots,(G_n,\circ_n)$都是群. 在 $G_1\times\cdots\times G_n$ 上规定，任意$(a_1,\cdots,a_n),(b_1,\cdots,b_n)\in G_1\times\cdots\times G_n$，对应

$$(a_1,\cdots,a_n)\otimes(b_1,\cdots,b_n)=(a_1\circ_1 b_1,\cdots,a_n\circ_n b_n).$$

则群$(G_1\times\cdots\times G_n,\otimes)$称为群$(G_1,\circ_1),\cdots,(G_n,\circ_n)$的**外直积**.

当各群之运算从上下文中能明确分辨出来时，可以不提运算，而简单说 $G_1\times\cdots\times G_n$ 是群 $G_1,\cdots,G_n$ 的外直积. 我们这里把群的外直积$(G_1\times\cdots\times G_n,\otimes)$记为 $G_1\otimes\cdots\otimes G_n$.

命题 2 如果 $G=\langle g\rangle$是 m 阶循环群，$H=\langle h\rangle$是 n 阶循环群，且 m,n 互质. 则 G 和 H 的外直积 $G\times H$ 是个 mn 阶的循环群.

证明 看 $G\times H$ 中元素(g,h)的阶数.

如果有正整数 k 使$(g,h)^k=(e_G,e_H)$，即

$$(g^k,h^k)=(e_G,e_H),$$

也就是 $g^k=e_G$，$h^k=e_H$，那么，因为 m 是 g 的阶数，n 是 h 的阶数，据 §4 命题 1，应有 $m|k$，$n|k$.

下面来证明 $(mn)|k$. 由于 $m|k$，设有整数 t 使 $k=mt$. 再由 m,n 互质，设有

$$pm+qn=1,\quad p,q\in \mathbf{I}.$$

于是，有

$$ptm+qtn=t,\quad pk+(qt)n=t.$$

由于 $n|k$，知道 n 整除上式左端两项，从而 n 应当整除 t. 设 $t=ns$，$s\in \mathbf{I}$，则

$$k=mt=mns,$$

即 $(mn)|k$.

这说明，只要 k 使得 $(g,h)^k=(e_G,e_H)$，则必有 $(mn)|k$. 而且

$$(g,h)^{mn}=(g^{mn},h^{mn})=(e_G,e_H),$$

即 mn 是使得 $(g,h)^k=(e_G,e_H)$ 成立之最小的非负整数. 据阶数的定义，(g,h) 的阶数为 mn.

很容易看出，当 G 的阶数为 m，H 的阶数为 n 时，$G\times H$ 的阶数为 mn.

现在，$\langle(g,h)\rangle$ 的阶数为 mn，故必有

$$G\times H=\langle(g,h)\rangle. \qquad \blacksquare$$

例题 1 设群 G 和群 H 的阶数均为 p，p 是个素数并可决定 G 和 H 的外直积 $G\otimes H$ 所含子群的个数.

解 $G\otimes H$ 阶数为 p^2. 由于 p 是个素数，p^2 只有 3 个因数，$1,p,p^2$. 从而 $G\otimes H$ 的子群的阶数只能是 $1,p,p^2$.

任何群的 1 阶子群只有一个，由恒等元生成. 任何有限群与自己阶数相等的子群也只有一个，即其本身.

现在，我们来计算 $G\otimes H$ 的 p 阶子群的个数.

首先，由拉格朗日定理的推论 3 知道，p 阶群（p 是素数）一定是循环群.

其次，任取 $G\otimes H$ 的一个不等于恒等元的元素 (g,h)，则由 G 和 H 的阶数为 p，知

$$(g,h)^p=(g^p,h^p)=(e_G,e_H).$$

同时，因为 (g,h) 不是 (e_G,e_H)，它的阶数不能为 1；也就是说，(g,h) 的阶数为 p. $G\otimes H$ 中非恒等元的阶数均为 p，从而它们生成的子群阶数亦为 p.

$G\otimes H$ 共有 p^2-1 个元素不为恒等元，它们各自生成一个 p 元循环群. 而每个循环群中含有 $p-1$ 个非恒等元. 也就是说，这 p^2-1 个元素生成的循环群中，每个循环群都重复出现 $p-1$ 次. 所以，$G\otimes H$ 中共有

$$(p^2-1)/(p-1)=p+1$$

个不同的 p 阶循环群.

$G\otimes H$ 的 p 阶子群都是循环群. 从而 $G\otimes H$ 有 $p+1$ 个 p 阶子群.

综合之，$G\otimes H$ 有 $p+3$ 个子群. ∎

设 G,H 是任意的两个群，$G\otimes H$ 是它们的外直积. 令

$$G'=\{(g,h)\in G\otimes H \mid h=e_H\},$$
$$H'=\{(g,h)\in G\otimes H \mid g=e_G\}.$$

换句话说，G' 是 $G\otimes H$ 的一个子集，它由 $G\otimes H$ 中 (g,e_H) 形式元素组成，g 取遍群 G. H' 是 $G\otimes H'$ 的一个子集，它由所有形如 (e_G,h) 的元素组成，h 取遍群 H.

命题 3 符号如上. 那么，G' 和 H' 都是 $G\otimes H$ 的子群.

证明 首先 $(e_G,e_H)\in G'$.

其次，任意 $(g_1,e_H),(g_2,e_H)\in G'$，则

$$(g_1,e_H)\otimes(g_2,e_H)=(g_1g_2,e_H)\in G',$$

即 G' 乘法封闭.

最后，对每个 $(g,e_H)\in G'$，有 $(g^{-1},e_H)\in G'$.

所以，G' 是 $G\otimes H$ 的一个子群. 同理，H' 也是 $G\otimes H$ 的一个

子群. ∎

命题 4 符号如上.那么 $G\otimes H$ 的每一个元素都是一个 G' 的元素和一个 H' 的元素的乘积,而且这两个元素可交换.如果不计次序,那么 $G\otimes H$ 的元素表成 G' 的元与 H' 的元之积时,表法唯一.

证明 任取 $(g,h)\in G\otimes H$,就有

$$(g,h)=(g,e_H)\otimes(e_G,h)=(e_G,h)(g,e_H),$$

其中 $(g,e_H)\in G'$, $(e_G,h)\in H'$.

如果有 $(g_1,e_H),(g_2,e_H)\in G'$, $(e_G,h_1),(e_G,h_2)\in H'$,且

$$(g_1,e_H)\otimes(e_G,h_1)=(g_2,e_H)\otimes(e_G,h_2),$$

即有

$$(g_1,h_1)=(g_2,h_2), \qquad (*)$$

作为集合,群 $G\otimes H$ 是集合 G 和 H 的笛卡尔积,$(*)$ 意味着 $g_1=g_2$, $h_1=h_2$.这就说明表法是唯一的. ∎

命题 5 符号如上.用 $\sim$ 代表 H' 在 $G\otimes H$ 中确定的右关系,则 G' 是 $\sim$ 关系之下等价类表示的一个完全集.

证明 如果 $(g_1,e_H),(g_2,e_H)\in G'$,

$$(g_1,e_H)\sim(g_2,e_H),$$

即 $(g_1,e_H)\otimes(g_2,e_H)^{-1}\in H'$,也就是

$$(g_1g_2^{-1},e_H)\in H'.$$

于是,应有 $g_1g_2^{-1}=e_G$, $g_1=g_2$.

这说明,G' 的不同的元素在不同的 $\sim$ 等价类中(每个等价类就是 $G\otimes H$ 关于 H' 的一个右陪集).

进一步,对任意 $(g,h)\in G\otimes H$,有

$$(g,h)\otimes(g^{-1},e_H)=(e_G,h)\in H',$$

也就是

$$(g,h)\sim(g,e_H), \quad (g,h)\in H'(g,e_H);$$

即 $G\otimes H$ 之每个元素必然属于某个 G' 中元素的右陪集中.

所以，G'是$G\otimes H$关于H'的右等价类表示的一个完全集合. ∎

例题 2 设Z是群G的中心，C是群H的中心，即

$$Z=\{x\in G \mid gx=xg,\text{对任意 } g\in G\},$$
$$C=\{y\in H \mid hy=yh,\text{对任意 } h\in H\}.$$

那么笛卡尔积$Z\times C$恰好是群$G\otimes H$的中心，即

$$Z\times C=\{(x,y)\in G\otimes H \mid (x,y)(g,h)=(g,h)(x,y),\ \text{任意 } g\in G,\ h\in H\}.$$

证明 若$(x,y)\in Z\times C$，即$x\in Z$，$y\in C$，那么对任意$g\in G$，$h\in H$都有

$$xg=gx,\quad yh=hy,$$

从而$(x,y)(g,h)=(g,h)(x,y)$.

反过来，若$(x,y)\in G\otimes H$，且对任意$g\in G$，$h\in H$都有

$$(x,y)(g,h)=(g,h)(x,y);$$

分开写，也就是

$$xg=gx,\quad yh=hy.$$

这说明$x\in Z$，$y\in C$，从而$(x,y)\in Z\times C$.

所以，

$$Z\times C=\{(x,y)\in G\otimes H \mid (x,y)(g,h)=(g,h)(x,y),\ \text{任意 } g\in G,\ h\in H\}.$$ ∎

习 题 六

1. 给出群$(\mathrm{I}_2,+)$，$(\mathrm{I}_3,+)$外直积$(\mathrm{I}_2,+)\otimes(\mathrm{I}_3,+)$的乘法表.
2. 给出$(1^*,1^*)$以外的元素，它也是上题中循环群$(\mathrm{I}_2,+)\otimes(\mathrm{I}_3,+)$的生成元.
3. 给出群$(\mathrm{I}_2,+)$的外直积$\mathrm{I}_2\otimes\mathrm{I}_2\otimes\mathrm{I}_2$的所有子群.

小 结

群，是抽象代数学中头号重要的概念.

数的加法、非奇异矩阵的乘法、可逆映射的复合、刚体的运动等表面上差别颇大的现象，本质上却可以抽象出相同的基础：一个集合上有个二元运算且满足§1之(1)，(2)和(3).

有了这个共同基础，经过严格的推理，我们知道，它们必有很多内在的深入的相同之处.例如消去律、恒等元唯一，等等.

这样，今后只要遇到一个带运算的集合满足(1)，(2)和(3)，即使是从来没遇见过的新科研成果中的对象，我们也不用重复推理而可直接判断，它必满足消去律.这就叫举一反三.这就叫公理化方法.

在公理(1)，(2)和(3)的基础上做形式推演绝不是文字游戏，这是给深入学习打基础.

读者必须对群的定义作最深入地研究，不是背诵定义的文字而是理解其实质.

要丢开书自己就能顺利地证明，对于一个集合 G 和 G 上的二元运算下列几组条件等价：

(1) 结合律， (2) 有恒等元， (3) 每元有逆元；

(1)′ 结合律， (2)′ 有左恒等元， (3)′ 每元有左逆元；

(1)″结合律， (2)″ 有唯一的恒等元， (3)″ 每元有唯一的逆元；

(1)‴ 结合律， (2)‴ 对任意 $a,b\in G$，方程

$$ax=b,\quad ya=b$$

恒有解.

要把握住群的实质，必须熟悉一些群的实例，如整数加群、$\mathbf{I}_n$ 加群、置换群、循环群.

子群这一概念接受起来应无困难，但对子群的陪集需多下工夫.下一章我们要把陪集做为元素去运算.众多陪集搅在一起令人眼花，读者最好在这里事先多观察观察它们.

有限群是个重要群类.拉格朗日定理叙述起来简单但能定量地给出群阶与子群阶的关系，是处理有限群结构的极有用的工具.

如能灵活运用常可事半而功倍.

关于外直积的讲述已经超过了自学考试大纲的要求.由于这个概念比较好接受,在构造群的例子的时候能开阔眼界,这里写成短短一节,不要求每位读者都仔细阅读,知道一点新思路是有好处的.

复 习 题

1. 设$(G,\cdot)$是个群.规定任意$a,b\in G$, $a*b=b\cdot a$.证明:$(G,*)$也是个数.

2. 在群G中已知$x^{-1}yx=y^{-1}$, $y^{-1}xy=x^{-1}$.求证:$x^4=y^4=e$.

3. 在群G中任取一固定元a,规定$f:g\to ag$, $g\in G$.证明:f是个双射

4. 设H是G的子群,S是G的所有关于H的左陪集的集合,T是G的所有关于H的右陪集的集合.则映射

$$\sigma:aH\to Ha^{-1},\quad a\in G$$

是S到T的双射.

5. 设G是个群,$a,b\in G$, b的阶数是3, $ab=ba$.那么a,b生成的子群$\langle a,b\rangle$的元素只能是下列三种形式元素之一:

$$a^i,ba^j,b^2a^l,\quad i,j,l\in \mathrm{I}.$$

6. 设$(H,+)$是整数加群$(\mathrm{I},+)$的子群,且$H\neq \mathrm{I}$.那么H必为全体偶数的集合.

7. 设G是个群,$a\in G$.证明:a^{-1}与a阶数相同.

8. 证明:有理数加群$(\mathrm{Q},+)$的每个非零元素的阶数都是无限的.

9*. 设G是个n元集合,$\cdot$是G上的一个满足结合律的二元运算.若它还满足左、右消去律,那么$(G,\cdot)$是个群.

第三章　群的同态

小孩子作加法，先把2个苹果与2个手指对应，3个苹果与3个手指对应；然后，计算2个手指加3个手指，数一下，得5个手指；最后，再根据对应原则判定，2个苹果加3个苹果也必然是5个苹果.

这就是本章要讨论的群的同构的思想背景. 把那些从代数学观点看来结构相同的群归成类，研究问题时即可举一反三.

另一个学习方法是把大的、复杂的群归结为对小的简单些的群的研究. 比如，要了解一个旅馆的各房间的布置情况，可以看一个小的模型，可知道，楼有几层，各房间的位置等，然后，再具体看各等级房间的代表，具体了解床、桌、电话的位置. 如果同等级房间内部都一样，那么，你用较少时间了解了整个旅馆.

这种研究方法用在群的研究上，我们要引人"群的同态"概念，并得到一系列深刻结果. 特别是群同态基本定理.

本章有些内容比较抽象. 相当多的初学者对"商群"等概念会觉得难于理解. 为此，各节都配有较多例题，读者不要轻易跳过去. 同时，也附有难易不同的习题，读者应尽量独立完成.

这一阶段是整个《抽象代数学》学习过程中思想方法上的一次飞跃，如果顺利通过本章各个环节，那么在其后的内容的学习上将不会有根本性障碍.

§1 群的同构

对于自然数,不同的民族发明了不同的计数方法,有{一,二,三,四,…},有{1,2,3,…}有{Ⅰ,Ⅱ,Ⅲ,…},也有{one,two,three,…}等等.但是,在数学上,我们认为它们是相同的系统,而符号上的差别是无关紧要的.因为只要经过一个翻释过程,任何一个系统中的运算成果都可以在其他系统使用.

这种只是符号不同而实质上(我们只注意其代数运算,与此无关的东西就认为是非实质性的)相同的系统是大量存在的.为此,引入"同构"的概念.

定义 1 设(G,Δ)是个群,$(H,\circ)$也是个群.如果$f:G\to H$是个双射,且对任意$a,b\in G$恒有

$$f(a\Delta b)=f(a)\circ f(b),$$

则说f是G到H的**同构映射**.如果有G到H的同构映射,就说(G,Δ)和$(H,\circ)$**同构**.有时简单地说G和H同构,或G同构于H.

例 1 阿拉伯数字的集合

$$\mathbf{I}=\{\cdots,-1,0,1,2,\cdots\}$$

在+运算之下是个群.

汉字的小写数字的集合

$$H=\{\cdots,负一,0,一,二,\cdots\}$$

在"加"运算之下也是个群.

规定$\mathbf{I}$到H的映射f,

$$f(1)=一,\ f(z)=二,\ \cdots,$$

即得群$(G,+)$到$(H,加)$的一个同构映射.群$(G,+)$和群$(H,加)$同构.

例 2 设$(\mathbf{I},+)$是整数加法群,$(E,+)$是偶数加法群.

规定,每个$m\in\mathbf{I}$对应$2m\in E$,这个映射记为f,即

$$f(m)=2m,\quad m\in\mathbf{I}.$$

这是个单射. 因为,当 $m \neq n$ 时

$$f(m)=2m \neq 2n=f(n).$$

这又是个双射. 因为 E 中每个元 l 必然是某个整数 k 的 2 倍,即 $l=2k=f(k)$, $k \in \mathbf{I}$.

同时,对任意 $m, n \in \mathbf{I}$,有

$$f(m+n)=2(m+n)=f(m)+f(n).$$

所以,f 是 $(\mathbf{I},+)$ 到 $(E,+)$ 的同构映射,$\mathbf{I}$ 同构于 E.

例 3 设 $(\mathbf{R}_+,\cdot)$ 是正实数的乘法群,而 $(\mathbf{R},+)$ 是实数加法群.

规定,任意正实数 $x \in \mathbf{R}_+$ 对应实数 $\lg x$,则得到 $\mathbf{R}_+$ 到 $\mathbf{R}$ 的一个映射,记为 f,即 $f(x)=\lg x$, $x \in \mathbf{R}_+$.

显然,f 是单射. 对任意 $y \in \mathbf{R}$,令 $x=10^y$,则 $x>0$, $x \in \mathbf{R}_+$,且

$$f(x)=\lg x=\lg 10^y=y,$$

即 f 为满射. 从而 f 是双射. 对任意 $a, b \in \mathbf{R}_+$,我们还有

$$\lg(a \cdot b)=\lg a+\lg b.$$

这就说明了 f 是 $(\mathbf{R}_+,\cdot)$ 到 $(\mathbf{R},+)$ 的同构映射.

例 4 对任意群 $(G,\circ)$ 而言,G 上的恒等映射 i_G 是群 $(G,\circ)$ 到群 $(G,\circ)$ 的同构映射.

例 5 回忆第一章 §6 的例 9. 看群 $(\mathbf{I}_3,+)$ 和 3 阶对称群的子群 $H=\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$. 它们的运算表是

$+$	0^*	1^*	2^*
0^*	0^*	1^*	2^*
1^*	1^*	2^*	0^*
2^*	2^*	0^*	1^*

$\circ$	(1)	(1 2 3)	(1 3 2)
(1)	(1)	(1 2 3)	(1 3 2)
(1 2 3)	(1 2 3)	(1 3 2)	(1)
(1 3 2)	(1 3 2)	(1)	(1 2 3)

只要让 $0^*, 1^*, 2*$ 分别对应 (1),(1 2 3),(1 3 2) 则很容易看出这是个同构映射.

例 6 我们知道,$\mathbf{I}_{13}$ 上有乘法运算(第一章 §6), $\mathbf{I}_{13}-\{0^*\}$ 在

此乘法之下是个群，它的子群 $G=\{1^*,5^*,8^*,12^*\}$ 与复数的乘法群 $H=\{1,-1,\mathrm{i},-\mathrm{i}\}$ 是同构的.

建立 G 到 H 的对应 f,

$$f(1^*)=1,\ f(5^*)=\mathrm{i},\ f(12^*)=-1,\ f(8^*)=-\mathrm{i},$$

即可.

读者可先想一下为什么能建立这样的对应，下面我们将给出更一般地关于循环群同构的结论.

命题 1 设 (G,Δ) 和 $(H,\circ)$ 是群，f 是 (G,Δ) 到 $(H,\circ)$ 的同构映射. 那么 $f(e_G)=e_H$.

证明 由于在 H 中，我们有

$$f(e_G)=f(e_G\Delta e_G)=f(e_G)\circ f(e_G),$$

用 $f(e_G)$ 的逆元乘等式两端，即得 $e_H=f(e_G)$. ▌

命题 2 条件如命题 1. 那么对于 G 中之任意元素 a，都有 $f(a^{-1})=f(a)^{-1}$. 其中 $f(a)^{-1}$ 即 H 中元素 $f(a)$ 的逆元.

证明 因为

$$f(a)\circ f(a^{-1})=f(a\Delta a^{-1})=f(e_G)=e_H,$$

所以 $f(a^{-1})$ 是 $f(a)$ 在 H 中的逆. 而群中任何元素的逆元素都是唯一的，故 $f(a^{-1})=f(a)^{-1}$. ▌

命题 3 设 $A=\{(G,\Delta),(H,\circ),(K,\#),\cdots\}$ 是由一些群构成的一个集合. 我们在 A 中定义关系 $\approx$, $(G,\Delta)\approx(H,\circ)$ 当而且仅当 G 同构 H. 那么，$\approx$ 是 A 上的等价关系.

证明 对任意 $(G,\Delta)\in A$, G 上的恒等映射 i_G 乃是群同构映射，故有 $(G,\Delta)\approx(G,\Delta)$. 即 $\approx$ 有反身性.

如果 $(G,\Delta)\approx(H,\circ)$, $(H,\circ)\approx(K,\#)$，设 f 是 G 到 H 的同构映射，g 是 H 到 K 的同构映射. 首先，$f:G\to H$, $g:H\to K$，则得映射

$$gf:G\to H.$$

由于 f 和 g 都是双射，从面 gf 是个双射. 其次，对任意 $a,b\in G$，有

$gf(a\Delta b)$

$=g[f(a\Delta b)]$ (映射复合的定义)

$=g[f(a)\circ f(b)]$ (f 是同构映射)

$=g[f(a)]\# g[f(b)]$ (g 是同构映射)

$=gf(a)\# gf(b).$ (映射合成的定义)

所以，gf 是 G 到 K 的同构映射. 即 $\approx$ 有传递性.

设 $(G,\Delta)\approx(H,\circ)$，$f$ 是 G 到 H 的同构映射，由于 f 是 G 到 H 的双射，所以它是可逆映射，即有 H 到 G 的映射 f^{-1}，对任意 $x\in H$，有

$$f^{-1}(x)=a,\quad f(a)=x.$$

而且 f^{-1} 也是双射. 进一步，任取 $x,y\in H$，则有 $a,b\in G$ 使

$$x=f(a),\quad y=f(b),\qquad (*)$$
$$a=f^{-1}(x),\quad b=f^{-1}(y).$$

故

$$f^{-1}(x\circ y)=f^{-1}(f(a)\Delta f(b)).$$

而 f 是同构映射，$f(a)\Delta f(b)=f(a\Delta b)$，所以，

$f^{-1}(x\circ y)$

$=f^{-1}[f(a\Delta b)]$ (f 是同构映射)

$=a\Delta b$ (f^{-1} 是 f 的逆)

$=f^{-1}(x)\Delta f^{-1}(y).$ (见 $(*)$ 式)

这说明 f^{-1} 是 H 到 G 的同构映射，$(H,\circ)\approx(G,\Delta)$，即关系 $\approx$ 有对称性.

总之，$\approx$ 是群之间的一个等价关系. ∎

这样，我们就可以把 G 同构于 H 说成 H 和 G 同构；G,H 同构等等.

命题 4 任意 n 阶循环群都同构于 $(\mathbf{I}_n,+)$.

证明 设 $(G,\cdot)$ 是元素 g 生成的 n 阶循环群，$G=\{e,g,\cdots,g^{n-1}\}$. 规定，G 中元素 g^i 对应 i^*，此映射记为 f，即

$$f(g^i)=i^*,\quad 0\leqslant i<n.$$

容易看出 f 是 G 到 $\mathbf{I}_n$ 的双射. 且

$$
\begin{aligned}
& f(g^i \cdot g^j) \\
& \quad = f(g^{i+j}) && \text{(循环群中元素乘的规律)} \\
& \quad = f(g)^{i+j} && \text{(f 是同构映射)} \\
& \quad = (i+j)1^* && \text{($\mathbf{I}_n$ 是交换群,变记法)} \\
& \quad = i^* + j^* && \text{($\mathbf{I}_n$ 的加法运算规律)} \\
& \quad = f(g^i) + f(g^j). && \text{(f 的定义)}
\end{aligned}
$$

所以, f 是 G 到 $(\mathbf{I}_n, +)$ 的同构映射. ▌

回过头来看例 5 和例 6. 由于 $\mathbf{S}_3$ 中

$$\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$$

是 3 阶循环群,它当然同构于 $(\mathbf{I}_3, +)$. 又由于

$$\{1, \mathrm{i}, -1, -\mathrm{i}\}$$

的乘群仍是 i 生成的 4 阶循环群,而

$$\{1^*, 5^*, 12^*, 8^*\}$$

是 5^* 生成的 4 阶循环群,它们也是同构的.

命题 5 任意无限循环群都同构于整数加法群 $(\mathbf{I}, +)$.

证明 设 $G = \langle g \rangle$ 是无限循环群. 建立 G 到 $\mathbf{I}$ 的对应 f,

$$f(g^i) = i, \ i \in \mathbf{I}.$$

由于 G 是无限阶的,当 $i \neq j$ 时, $g^i \neq g^j$,故对每个 $g^i \in G$, i 是唯一确定的, f 是 G 到 $\mathbf{I}$ 的映射. 对任意 $j \in \mathbf{I}$ 都有

$$f(g^j) = j,$$

所以, f 是个满射. 另一方面, 如果 $g^i \neq g^j$, 当然有 $i \neq j$, 也就是 $f(g^j) \neq f(g^i)$. 所以, f 还是个单射. 从而 f 是个双射. 进而, 对任意 $g^i, g^j \in G$, 都有

$$
\begin{aligned}
& f(g^i \cdot g^j) \\
& \quad = f(g^{i+j}) && \text{(循环群中乘法规律)} \\
& \quad = i + j && \text{(f 的定义)} \\
& \quad = f(g^i) + f(g^j). && \text{(f 的定义)}
\end{aligned}
$$

即 f 是个同构映射. ∎

关于命题 4 和命题 5,其反面问题亦可解决,即

命题 6 设群(G,Δ)同构于群$(H,\circ)$,而 G 是个循环群,则 H 也是循环群.

事实上,如果 g 是 G 的生成元,f 是 G 到 H 的映射,则 $f(g)$ 必为 H 的生成元.

这是因为,对任意 $x\in H$,由于 f 是满射,必有 G 中元 $a=g^i$,使得

$$f(a)=f(g^i)=x.$$

而 f 是同构映射,故当 $i\geqslant 0$ 时

$$f(g^i)=[f(g)]^i;$$

而当 $i\leqslant 0$ 时 $g^i=(g^{-i})^{-1}$. 由命题 1 知

$$f(g^i)=f(g^{-i})^{-1}.$$

而 $-i\geqslant 0$,与上面一样$(-i)$个相乘后在 f 之下对应的 $f(g^{-i})$等于$(-i)$个 $f(g)$相乘,即

$$f(g^{-i})=f(g)^{-i}.$$

从而有

$$f(g^i)=f(g^{-i})^{-1}=[f(g)^{-i}]^{-1}=f(g)^i. \qquad ∎$$

总之,有 $x=f(g)^i$. 所以,$f(g)$是 H 的生成元.

由于群之间的同构映射首先是集合间的双射,所以同构的群的阶数相同.(当它们是有限集时,其所含元素的数目相同;当它们是无限集时,能在它们之间建立双射,从集合论观点看,它们元数也认为相同.)

例题 1 群$(\mathbf{I}_{13}-\{0^*\},\cdot)$的子群 $G=\{1^*,5^*,8^*,12^*\}$和群$(\mathbf{I}_{12}-\{0^*\},\cdot)$的子群 $H=\{1^*,5^*,7^*,11^*\}$不能同构.

证明 要说明两个群(G,Δ)和$(H,\circ)$不同构,就要说明 G 到 H 的任何映射 f,不能同时满足两个条件

(1) f 为双射;

(2) 对任意 $a,b\in G$ 都有 $f(a\Delta b)=f(a)\circ f(b)$. 也等于

说,上述两个条件有一个成立时,则另一个一定不成立.所以,G不同构于H的等价说法还有

(1°) 如果f是G到H的双射,那么必定有某一对$a,b\in G$,

$$f(a\Delta b)\neq f(a)\circ f(b).$$

(2°) 如果f是G到H的映射,且对任意$a,b\in G$都有$f(a\Delta b)=f(a)\circ f(b)$,则$f$必定不是双射.

这些说法各有方便之处,在处理不同问题时,适当选择之,可使证明显得简洁.

回到该例题本身.设f是G到H的一个同构映射,然后推出矛盾.

5^*是G的生成元,其阶数为4.由命题6知$f(5^*)\in H$应该是H的生成元.但H不是循环群,它的元素最高阶数为2. ▌

命题7* 设(G,Δ),$(H,\circ)$和$(K,\#)$是任意群,$(G\times H,\otimes_1)$是G和H的外直积,而

$$((G\times H)\times K,\otimes_2)$$

是$(G\times H,\otimes_1)$和$(K,\#)$的外直积.同时,群

$$(G\times H\times K,\otimes_3)$$

是G,H,K的外直积.那么$((G\times H)\times K,\otimes_2)$同构于

$$(G\times H\times K,\otimes_3).$$

证明 建立笛卡尔积$(G\times H)\times K$到$G\times H\times K$的映射f,对任意$a\in G$, $u\in H$, $x\in K$,

$$f(((a,u),x))=(a,u,x).$$

这是个双射.

进一步,对任意$((a,u),x)$,$((b,v),y)\in(G\times H)\times K$,我们都有

$$\begin{aligned}&f(((a,u),x)\otimes_2((b,v),y)\\&=f((a,u)\otimes_1(b,v),x\#y) &&(\otimes_2\text{ 的定义})\\&=f((a\Delta b,u\circ v),x\#y) &&(\otimes_1\text{ 的定义})\end{aligned}$$

$$=(a\Delta b, u\circ v, x\# y) \qquad (f\text{ 的定义})$$
$$=(a,u,x)\otimes_3(b,v,y) \qquad (\otimes_3\text{ 的定义})$$
$$=f(((a,u),x))\otimes_3 f(((b,v),y)). \qquad (f\text{ 的定义})$$

所以，f 是同构映射. ∎

例题 2 设 H 是所有形如

$$2^m 3^n,\quad m,n\in \mathbf{I}$$

的有理数在数的乘法之下构成的群，$\mathbf{I}\otimes\mathbf{I}$ 是整数加法群 $\mathbf{I}$ 和整数加法群 $\mathbf{I}$ 的外直积. 那么，$\mathbf{I}\otimes\mathbf{I}$ 同构于 H.

证明 定义 $\mathbf{I}\otimes\mathbf{I}$ 到 H 上的映射 f，对任意 $(m,n)\in\mathbf{I}\otimes\mathbf{I}$，

$$f((m,n))=2^m 3^n.$$

容易看出，f 是满射. 进一步，如果有 $(m,n),(p,q)\in\mathbf{I}\otimes\mathbf{I}$，且

$$2^m 3^n=2^p 3^q.$$

将其两端同乘一数 $2^k 3^l$ 使得

$$2^{m+k}3^{n+l}=2^{p+k}3^{q+l},$$

而且 $m+k, n+l, p+k, q+l$ 均大于 0. 由整数的素数分解的唯一性，必有

$$m+k=p+k,\quad n+l=q+l,$$

也就是 $m=p, n=q$. 这说明 f 是单射.

对任意 $(m,n),(i,j)\in\mathbf{I}\otimes\mathbf{I}$，

$$f((m,n)\otimes(i,j))$$
$$=f((m+i,n+j)) \qquad (\otimes\text{的定义})$$
$$=2^{m+i}\cdot 3^{n+j} \qquad (f\text{ 的定义})$$
$$=2^m 3^n 2^i 3^j \qquad (\text{数乘有交换性、结合性})$$
$$=f((m,n)\cdot f((i,j)). \qquad (f\text{ 的定义})$$

所以，f 是同构映射. ∎

例题 3 在第二章 §6 的例 2 中，所有 n 阶实的可逆矩阵在矩阵乘法之下的群 G，所有 m 阶实的可逆矩阵在矩阵乘法之下的群 H，导出它们的外直积 $G\otimes H$. 于是，群 G 同构于所有实的 $m+n$ 阶的可逆分块矩阵

$$\begin{pmatrix} A & 0 \\ 0 & X \end{pmatrix} \begin{matrix} n\text{ 行} \\ m\text{ 行} \end{matrix}$$

$$n\text{ 行}\ m\text{ 行}$$

在矩阵乘法之下构成的群 K.

事实上,规定 $G\otimes H$ 到 K 的映射 f,

$$f((A,X))=\begin{pmatrix} A & 0 \\ 0 & X \end{pmatrix}, \quad A\in G,\ X\in H.$$

则 f 是个双射,且对任意 $A,B\in G$, $X,Y\in H$ 有

$$\begin{aligned}
&f((A,X)\otimes(B,Y)) \\
&=f((AB,XY)) && \text{(外直积的定义)} \\
&=\begin{pmatrix} AB & 0 \\ 0 & XY \end{pmatrix} && (f\text{ 的定义}) \\
&=\begin{pmatrix} A & 0 \\ 0 & X \end{pmatrix}\begin{pmatrix} B & 0 \\ 0 & Y \end{pmatrix} && \text{(矩阵分块乘性质)} \\
&=f((A,X))f((B,Y)). && (f\text{ 的定义})
\end{aligned}$$

这就证明 $G\otimes H$ 和 K 是同构的. ▌

本节最后,让我们回忆一下第一章 §5 关于任意有限集上置换的定义. 在讨论任意集合 A 上置换和 $\{1,2,\cdots,n\}$ 上置换时说了一段现在看来不够精确的话. 这里,用同构术语来处理,就有

命题 8 设 A 是有 n 个元素的集合, G 是 A 到 A 的所有可逆映射在映射合成之下作成的群. 那么 G 同构于 $\mathbf{S}_n$.

证明 设 $A=\{a_1,a_2,\cdots,a_n\}$. 对 A 到 A 的任意一个可逆变换 π, 设

$$\pi(a_1)=a_{i_1},\ \cdots,\ \pi(a_n)=a_{i_n}$$

并记成

$$\pi=\begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ \pi(a_1) & \pi(a_2) & \cdots & \pi(a_n) \end{bmatrix},$$

或者

$$\pi=\begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ a_{i_1} & a_{i_2} & \cdots & a_{i_n} \end{bmatrix}.$$

由于 π 是双射，$a_{i_1},\cdots,a_{i_n}$ 两两不同，且每个 $a_j(j=1,2,\cdots,n)$ 必然出现一次，所以数码 $i_1,\cdots,i_n$ 两两不同，$i_1,\cdots,i_n$ 是 $1,2,\cdots,n$ 的一个排列；也就是说

$$\pi^*=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}$$

是集合 $\{1,2,\cdots,n\}$ 上的一个置换.

对任意 $\pi\in G$，令 π 对应 π^*，则得到群 G 到群 $\mathbf{S}_n$ 的一个双射 f，$f(\pi)=\pi^*$.

对任意 $\pi,\ \rho\in G$，可将其写成如下形式

$$\pi=\begin{pmatrix}a_{i_1} & a_{i_2} & \cdots & a_{i_n}\\ a_{j_1} & a_{j_2} & \cdots & a_{j_n}\end{pmatrix},$$

$$\rho=\begin{pmatrix}a_1 & a_2 & \cdots & a_n\\ a_{i_1} & a_{i_2} & \cdots & a_{i_n}\end{pmatrix}.$$

于是

$$\pi\circ\rho=\begin{pmatrix}a_1 & a_2 & \cdots & a_n\\ a_{j_1} & a_{j_2} & \cdots & a_{j_n}\end{pmatrix}.$$

同时，有

$$f(\pi)=\pi^*=\begin{pmatrix}i_1 & i_2 & \cdots & i_n\\ j_1 & j_2 & \cdots & j_n\end{pmatrix},$$

$$f(\rho)=\rho^*=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix},$$

$$f(\pi\circ\rho)=\begin{pmatrix}1 & 2 & \cdots & n\\ j_1 & j_2 & \cdots & j_n\end{pmatrix},$$

恰好有 $f(\pi\circ\rho)=f(\pi)\circ f(\rho)$.

所以，f 是 G 到 $\mathbf{S}_n$ 的同构映射. G 同构于 $\mathbf{S}_n$. ∎

例题 4 如果群 G 的阶数为 4，但任何元素的阶数均不为 4，把 $(\mathbf{I}_2,+)$ 简记为 $\mathbf{I}_2$，则 $G\approx\mathbf{I}_2\otimes\mathbf{I}_2$.

证明 设 G 的元素是 e,a,b,c,其中 e 是 G 的恒等元.由拉格朗日定理知,G 的每个元素的阶数均能整除 4,而它们的阶都不为 4,故各元素的阶数只能为 1(恒等元 e)或为 2(元素 a,b 和 c).从而,对任意 $x\in G$,都有 $x^2=e$.

对任意 $x,y\in G$,又应有

$$(xy)^2=xyxy=e,\quad xy=y^{-1}x^{-1}.$$

但 $x^2=e,x=x^{-1}$,同样 $y=y^{-1}$,上式说明

$$xy=yx,\quad 对任意\ x,y\in G,$$

即 G 为交换群.

对任意 $x,y\in G$,若 $xy=x$,则推出 $y=e$,故当 x,y 为不同的非恒等元时 $xy\neq x$, $xy\neq y$,而且 $xy\neq e$,因为 x 的逆是 x 自己.这说明 xy 只能是另外一个非恒等元.

我们可列出 G 的乘法表

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(这样的群称为**克莱因**(Klein)**四元群**).而 $\mathbf{I}_2\otimes\mathbf{I}_2$ 的乘法是

$\otimes$	$(0^*,0^*)$	$(0^*,1^*)$	$(1^*,0^*)$	$(1^*,1^*)$
$(0^*,0^*)$	$(0^*,0^*)$	$(0^*,1^*)$	$(1^*,0^*)$	$(1^*,1^*)$
$(0^*,1^*)$	$(0^*,1^*)$	$(0^*,0^*)$	$(1^*,1^*)$	$(1^*,0^*)$
$(1^*,0^*)$	$(1^*,0^*)$	$(1^*,1^*)$	$(0^*,0^*)$	$(0^*,1^*)$
$(1^*,1^*)$	$(1^*,1^*)$	$(1^*,0^*)$	$(0^*,1^*)$	$(0^*,0^*)$

只要令 e,a,b,c 分别对应

$$(0^*,0^*),(0^*,1^*),(1^*,0^*),(1^*,1^*)$$

就得到 G 到 $\mathbf{I}_2\otimes\mathbf{I}_2$ 的一个同构映射. ▌

例题 5 设群 G 是由非恒等元不同的 a,b 两个元素生成的,

且 $aa=e, bbb=e, ab=b^2a$. 证明：G 同构于对称群 $\mathbf{S}_3$.

证明 先看 G 中有哪些不同的元素. 除 e, a, b 外，若 $b^2=1$，则 $b^3=b^2b=b=e$，矛盾；若 $b^2=b$，亦有 $b=e$ 矛盾；若 $b^2=a$，则 $b^4=e$，从而 $bb^3=b=e$，亦为矛盾. 所以，e, a, b, b^2 两两不同.

若 $ab=e$，由 $aa=e$ 可推出 $a=b$ 矛盾；若 $ab=b$ 则 $a=e$；若 $ab=a$ 则 $b=e$ 均有矛盾；若 $ab=b^2$ 亦推出 $a=b$，矛盾. 故 ab 异于 e, a, b, b^2.

同理 ba 与 e, a, b, b^2 均不等. 若 $ab=ba$，由 $ab=b^2a$ 推出 $b=e$，为一矛盾.

所以 e, a, b, b^2, ab, ba 是不同的 6 个元素. 为了说明它们乘起来封闭，列表

	e	a	b	b^2	ab	ba
e	e	a	b	b^2	ab	ba
a	a	e	ab	ba	b	b^2
b	b	ba	b^2	e	a	ab
b^2	b^2	ab	e	b	ba	a
ab	ab	b^2	ba	a	e	b
ba	ba	b	a	ab	b^2	e

这里只要注意 $b^2a=ab$，$(ab)a=b^2a^2=b^2$，$b(ab)=b^3a=a$，$(ab)b=(bba)b=ba$.

而且上乘法表说明 G 的运算由题设之三条件完全确定.

在 $\mathbf{S}_3$ 中，令 $a=(1\ 2)$，$b=(1\ 2\ 3)$，则亦有

$$aa=e, \quad bbb=e, \quad ab=bba=(2\ 3).$$

故 $\mathbf{S}_3$ 与 G 有相同之乘法表，$\mathbf{S}_3$ 与 G 同构. ▌

下面的例题虽然简单，但这种思想在第四章和第七章要反复出现.

例题 6 设 $f: A\to B$ 是集合 A 到集合 B 的一个双射，同时 $(A, \cdot)$ 是个群. 那么，在 B 上规定，任意 $x, y\in B$ 对应

$$f(f^{-1}(x)\cdot f^{-1}(y)),$$

则得到 B 上的一个二元运算,记为 $*$,即

$$x*y=f(f^{-1}(x)\cdot f^{-1}(y)).$$

证明:$(B,*)$构成群,而且 f 是群同构映射.

分析 由于 f 是双射,它有逆映射 f^{-1},因此 $x*y$ 是由 x,y 唯一确定的.

验证时一定要分清哪些运算是在 B 中进行,哪些运算是在 A 中进行.

证明 任取 $x,y,z\in B$,

$$\begin{aligned}
&(x*y)*z\\
&=f(f^{-1}(x)\cdot f^{-1}(y))*z && (*\text{的定义})\\
&=f\{[f^{-1}f(f^{-1}(x)\cdot f^{-1}(y))]\cdot f^{-1}(z)\} && (*\text{的定义})\\
&=f[(f^{-1}(x)\cdot f^{-1}(y))\cdot f^{-1}(z)] && (f^{-1}f\text{是恒等映射})\\
&=f\{f^{-1}(x)\cdot[f^{-1}(y)\cdot f^{-1}(z)]\} && (\text{运算}\cdot\text{是结合的})\\
&=f\{f^{-1}(x)\cdot f^{-1}f[f^{-1}(y)\cdot f^{-1}(z)]\} && (f^{-1}f\text{是恒等映射})\\
&=x*(y*z). && (*\text{的定义})
\end{aligned}$$

设 e 是$(A,\cdot)$的恒等元,那么对任意 $x\in B$,有

$$\begin{aligned}
&x*f(e)\\
&=f(f^{-1}(x)\cdot f^{-1}f(e)) && (*\text{的定义})\\
&=f(f^{-1}(x)\cdot e) && (f^{-1}f\text{是恒等映射})\\
&=f(f^{-1}(x)) && (e\text{是}A\text{的恒等元})\\
&=x. && (ff^{-1}\text{是恒等映射}).
\end{aligned}$$

这说明 $f(e)$是 B 的右恒等元.

下面先插进来证明 f 是保运算的,

任取 $u,v\in A$,则 $f(u),f(v)\in B$. 由于 f 是双射,知 $u=f^{-1}(x)$, $v=f^{-1}(y)$. 于是

$$\begin{aligned}
&f(u\cdot v)\\
&=f(f^{-1}(x)\cdot f^{-1}(y)) && (*\text{的定义})\\
&=x*y\\
&=f(u)*f(v).
\end{aligned}$$

接着再来证明对于任意 $x\in B$，x 必有右逆元.

由于 $f^{-1}(x)\in A$，A 是个群,从而必有 $v\in A$ 使 $f^{-1}(x)\cdot v=e$. 于是

$$f(f^{-1}(x)\cdot v)=f(e),\quad ff^{-1}(x)*f(v)=f(e),$$

也就是 $x*f(v)=f(e)$.

于是知$(B,*)$是个群,f 是$(A,\cdot)$到$(B,*)$的保运算的双射,f 是群同构. ▌

B 好像是 A 的影子,完全随着 A 的运算而运算.

习 题 一

1. 设 G 是个群,取定 $a\in G$,规定任意 x 对应 axa^{-1},得映射 $f:x\to axa^{-1}$. 证明:f 是 G 到 G 同构映射(通常称为是由 a 导出的内自同构).

2. 设 f 是群 G 到自己的同构映射(通常称为自同构. 证明:$H=\{g\in G;f(g)=g\}$ 是 G 的一个子群.

3. 设 G 是个群,Z 是 G 的中心,即

$$Z=\{g\in G\mid xg=gx,\text{对任意 } g\in G\}.$$

证明:$g\in Z$ 的充分必要条件是对任意一内自构 f 恒有 $f(g)=g$.

4*. 若群 G 之自同构都是恒等自同构,那么 G 的元素的阶数不大于 2.

5. 对于有理数加群$(\mathbf{Q},+)$,任意选定一个非零有理数 a,规定,每个有理数 x 对应有理数 ax,即 $f:x\to ax$. 则 f 是$(\mathbf{Q},+)$的一个自同构. 进一步证明:群$(\mathbf{Q},+)$的每个自同构必然都是某个有理数按上法导出的.

6. 给出例子:G 和 H 都是群,G 同构于 H 的一个真群,同时 H 又同构于 G 的一个真子群.

7. 证明:$\mathbf{S}_4$ 的子群$\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$同构于 $\mathbf{I}_2\times\mathbf{I}_2$. 再证明:矩阵

$$\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\0&-1\end{pmatrix},\begin{pmatrix}-1&0\\0&1\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$$

在矩阵乘法之下构成群且同构于 $\mathbf{I}_2\times\mathbf{I}_2$.(它们都可称为克莱因四元群).

§2 群上的可逆变换

在第一章§6,我们讨论过任意非空集合 A 到自己的所有可

逆映射的集合 $I(A)$. 后来,在第二章 §1 中,作为例 6,证明了 $I(A)$ 在映射的复合运算之下构成群.

当 A 是个有限集时,$I(A)$ 就是 A 上的对称群. 关于置换群的性质,读者已经有了初步了解.

这一节要讨论群 G 上的所有可逆映射在映射合成之下构成的群 $I(G)$ 的性质. 最重要的结果是,任意群必同构于其上可逆映射构成的群的一个子群.

一般的群,由于背景各异而千差万别,有了如上的"表示定理",我们只要把群上可逆映射所构成的群讨论充分,则其他出之各处的群也就清楚了.

定义 1 设 $(G,\cdot)$ 是个群,将 G 到 G 的可逆映射称为 G 上**可逆变换**. G 上所有可逆变换在映射合成之下构成群,记为 $I(G)$.

群 G 到 G 本身的同构映射称为 G 的**自同构**.

命题 1 G 的所有自同构的集合 $\mathrm{Aut}(G)$ 是 $I(G)$ 的一个子群.

实际上,若 $f:G\to G$, $g:G\to G$ 是同构映射,则 $f\circ g:G\to G$ 也是同构映射,即 $f\circ g$ 是 G 的自同构,$f\circ g\in\mathrm{Aut}(G)$.

若 $f:G\to G$ 是同构映射,则它的逆映射 f^{-1} 是 G 到 G 的同构映射;即 $f\in\mathrm{Aut}(G)$,则 $f^{-1}\in\mathrm{Aut}(G)$.

G 上的恒等映射 i_G 是自同构映射.

所以,$\mathrm{Aut}(G)$ 是 $I(G)$ 的子群. ∎

例题 1 决定群 $(\mathbf{I}_4,+)$ 的所有可逆变换构成的群 $I(\mathbf{I}_4)$ 和所有自同构构成的群 $\mathrm{Aut}(G)$.

解 $\mathbf{I}_4$ 上的所有可逆变换,就是 $\mathbf{I}_4$ 上的所有置换,它有 24 个元素,如

$$\begin{pmatrix}0^* & 1^* & 2^* & 3^*\\0^* & 1^* & 2^* & 3^*\end{pmatrix},\quad\begin{pmatrix}0^* & 1^* & 2^* & 3^*\\0^* & 1^* & 3^* & 2^*\end{pmatrix},$$

$$\begin{pmatrix}0^* & 1^* & 2^* & 3^*\\1^* & 0^* & 3^* & 2^*\end{pmatrix},\quad\begin{pmatrix}0^* & 1^* & 2^* & 3^*\\1^* & 2^* & 3^* & 0^*\end{pmatrix}$$

等等.

在这些置换中,只有把 0^* 变成 0^* 者才有可能是自同构,因为同构映射把恒等元(这里的 0^*)变成恒等元.

$\mathbf{I}_4$ 有两个生成元 1^* 和 3^*,同构映射必须把生成元变成生成元.

如果 f 是 $\mathbf{I}_4$ 到 $\mathbf{I}_4$ 的自同构.则必有

$$f(0^*)=0^*,$$

且 $f(1^*)=1$ 或 $f(1^*)=3^*$. 若 $f(1^*)=1^*$,则由于 f 是同构,必有

$$f(2^*)=f(1^*+1^*)=f(1^*)+f(1^*)=1^*+1^*=2^*,$$

$$f(3^*)=f(1^*+2^*)=f(1^*)+f(2^*)=1^*+2^*=3^*.$$

从而 f 为恒等映射.

若 $f(1^*)=3^*$,那么

$$f(2^*)=f(1^*)+f(1^*)=3^*+3^*=2^*,$$

$$f(3^*)=f(1^*)+f(2^*)=3^*+2^*=1^*,$$

即

$$f=\begin{pmatrix}0^* & 1^* & 2^* & 3^*\\ 0^* & 3^* & 2^* & 1^*\end{pmatrix}.$$

所以,Aut($\mathbf{I}_4$)是个 2 阶群,

$$\mathrm{Aut}(\mathbf{I}_4)=\left\{i_G,\begin{pmatrix}0^* & 1^* & 2^* & 3^*\\ 0^* & 3^* & 2^* & 1^*\end{pmatrix}\right\}.$$ ∎

命题 2 设 G 是个群,a 是 G 的一个固定元素. 通过 a 可以得到 G 上的一个变换 λ_a,规定每个 $x\in G$ 对应 ax,即

$$\lambda_a(x)=ax,\quad x\in G.$$

则 λ_a 是 G 上的可逆变换,称为 a **左乘变换**.

证明 由于 G 是个群,满足消去律,故对任意 $x,y\in G$,由

$$\lambda_a(y)=ay=ax=\lambda_a(x),$$

可推出 $y=x$,从而知道 λ_a 是个单射.

另一方面，对任意 $g\in G$，我们都有

$$g=aa^{-1}g=\lambda_a(a^{-1}g),$$

这说明 λ_a 是个满射.

总之，λ_a 是个双射，是可逆变换，$\lambda_a\in I(G)$. ▌

例 1 在 $(\mathbf{I},+)$ 中，整数 2 和 -7 所确定的可逆变换 λ_2 和 λ_{-7} 为

$$\lambda_2(m)=m+2,\ \lambda_{-7}(m)=m-7,\ m\in\mathbf{I}.$$

例 2 在 3 阶对称群 $\mathbf{S}_3$ 中，取 $a=(1\ 2)$，则

$$\lambda_a((1))=(1\ 2),\quad \lambda_a((1\ 2))=(1),$$
$$\lambda_a((1\ 3))=(1\ 3\ 2),\quad \lambda_a((2\ 3))=(1\ 2\ 3),$$
$$\lambda_a((1\ 2\ 3))=(2\ 3),\quad \lambda_a((1\ 3\ 2))=(1\ 3).$$

命题 3 设 G 是个群，G 中元素的所有左乘变换的集合 $L=\{\lambda_a\mid a\in G\}$ 是 $I(G)$ 的一个子群.

证明 设 e 是 G 的恒等元，则

$$\lambda_e(x)=ex=x,\quad x\in G,$$

即 $\lambda_e=i_G\in I(G)$.

对任意 $\lambda_a,\lambda_b\in L$，$a,b\in G$，由于

$$(\lambda_a\circ\lambda_b)(x)=\lambda_a(\lambda_b(x))=abx=\lambda_{ab}(x)$$

知 $\lambda_a\circ\lambda_b=\lambda_{ab}\in I(G)$.

对任意 $\lambda_a\in L$，$a\in G$，由

$$(\lambda_a\circ\lambda_{a^{-1}})(x)=aa^{-1}x=x=i_G(x),$$

知道 $\lambda_a\circ\lambda_{a^{-1}}=i_G$，即 $\lambda_{a^{-1}}$ 是 λ_a 的逆，而且 $\lambda_{a^{-1}}\in L$.

所以，L 是 $I(G)$ 的一个子群. ▌

例题 2 设 G 是 3 阶对称群 $\mathbf{S}_3$. 求 L.

解 利用第二章 §3 例 1 所给出的 $\mathbf{S}_3$ 的乘法表，可以看出 L 中 6 个元素是

$$\lambda_{P_1}=\begin{pmatrix}P_1 & P_2 & P_3 & P_4 & P_5 & P_6\\ P_1 & P_2 & P_3 & P_4 & P_5 & P_6\end{pmatrix},$$

$$\lambda_{P_2}=\begin{pmatrix}P_1 & P_2 & P_3 & P_4 & P_5 & P_6\\ P_2 & P_1 & P_6 & P_5 & P_4 & P_3\end{pmatrix},$$

$$\lambda_{P_3}=\begin{pmatrix}P_1 & P_2 & P_3 & P_4 & P_5 & P_6\\ P_3 & P_5 & P_1 & P_6 & P_2 & P_4\end{pmatrix},$$

$$\lambda_{P_4}=\begin{pmatrix}P_1 & P_2 & P_3 & P_4 & P_5 & P_6\\ P_4 & P_6 & P_5 & P_1 & P_3 & P_2\end{pmatrix},$$

$$\lambda_{P_5}=\begin{pmatrix}P_1 & P_2 & P_3 & P_4 & P_5 & P_6\\ P_5 & P_3 & P_4 & P_2 & P_6 & P_1\end{pmatrix},$$

$$\lambda_{P_6}=\begin{pmatrix}P_1 & P_2 & P_3 & P_4 & P_5 & P_6\\ P_6 & P_4 & P_2 & P_3 & P_1 & P_5\end{pmatrix}.$$

我们早已说过,既然每个元素都有字母 P,现可将其都去掉,即令 P_i 对应 i,则 L_{P_i} 对应 S_6 中的置换

$$(1),\qquad (1\ 2)(3\ 6)(4\ 5),$$
$$(1\ 3)(2\ 5)(4\ 6),\qquad (1\ 4)(2\ 6)(3\ 5),$$
$$(1\ 5\ 6)(2\ 3\ 4),\qquad (1\ 6\ 5)(2\ 4\ 3).$$

即 L 同构于 $\mathbf{S}_6$ 的由上述 6 个元素构成的子群 L^*. ▎

命题 4 设 G 为任意一个群,L 是其元素导出的所有左乘变换形成的群,则 G 同构于群 L.

证明 定义群 G 到群 L 的映射 f, $f(a)=\lambda_a$, $a\in G$.

先来说明 f 是个双射.若 $a,b\in G$, $a\neq b$,则 $ae\neq be$, $\lambda_a(e)\neq\lambda_b(e)$.但两个映射相等的充分必要条件是它们对 G 的每个元都作用都相同,故 $\lambda_a\neq\lambda_b$;从而

$$f(a)=\lambda_a\neq\lambda_b=f(b),$$

这说明 f 是个单射.

另一方面,L 中的每个元素 λ_a 必是 G 中元素导出的一个左乘

变换,同时

$$f(a)=\lambda_a,$$

所以,f 还是个满射.

进一步,可以证明,对任意 $a,b\in G$,都有

$$f(ab)=f(a)\circ f(b).$$

因为这是一个映射的等式,我们只要证明等式左端映射和右端映射作用在 G 的每个元素上结果相同.

对任意 $x\in G$,有

$f(ab)(x)$

$=\lambda_{ab}(x)$ （f 的定义）

$=(ab)x$ （λ_{ab} 的定义）

$=a(bx)$ （G 中有结合律）

$=\lambda_a(bx)$ （λ_a 的定义）

$=\lambda_a(\lambda_b(x))$ （λ_b 的定义）

$=(\lambda_a\circ\lambda_b)(x)$ （映射合成的定义）

$=(f(a)\circ f(b))(x)$ （f 的定义）

所以,$f(ab)=f(a)\circ f(b)$.

这就证明了,G 同构于 L. ▍

综合命题 2、命题 3 和命题 4,即得著名的**凯莱(Cayley)定理**如下:

定理 每个群 G 都同构于其上所有可逆变换作成的群 $I(G)$ 的一个子群. ▍

推论 每个 n 阶有限群必同构于 n 阶对称群 $\mathbf{S}_n$ 的一个子群.

事实上,设 G 是 n 阶群,那么 G 上的可逆变换即称为 G 上置换,由上节之命题 8 知道,A 上所有置换作成的群 H 同构于 $\{1,2,\cdots,n\}$ 上的置换群 $\mathbf{S}_n$. 由凯莱定理推出 G 同构于 H 的一个子群,从而 G 同构于 $\mathbf{S}_n$ 的一个子群. ▍

凯莱定理表明，任意群都同构于可逆变换群的一个子群. 对于变换群，特别是置换群，我们比较熟悉. 这样，就可以用熟悉的东西来解释还不熟悉的东西.

这种让任意群的每个元素都(同构地)对应一个可逆变换的作法，可以说是给任意群一个变换表示.

例题 3 给出群$(\mathbf{I}_5, +)$的置换表示.

解 按前面给的符号做，有

$$0^* \to \lambda_{0^*} = \begin{bmatrix} 0^* & 1^* & 2^* & 3^* & 4^* \\ 0^* & 1^* & 2^* & 3^* & 4^* \end{bmatrix} \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix},$$

$$1^* \to \lambda_{1^*} = \begin{bmatrix} 0^* & 1^* & 2^* & 3^* & 4^* \\ 1^* & 2^* & 3^* & 4^* & 5^* \end{bmatrix} \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix},$$

$$2^* \to \lambda_{2^*} = \begin{bmatrix} 0^* & 1^* & 2^* & 3^* & 4^* \\ 2^* & 3^* & 4^* & 0^* & 1^* \end{bmatrix} \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix},$$

$$3^* \to \lambda_{3^*} = \begin{bmatrix} 0^* & 1^* & 2^* & 3^* & 4^* \\ 3^* & 4^* & 0^* & 1^* & 2^* \end{bmatrix} \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix},$$

$$4^* \to \lambda_{4^*} = \begin{bmatrix} 0^* & 1^* & 2^* & 3^* & 4^* \\ 4^* & 0^* & 1^* & 2^* & 3^* \end{bmatrix} \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}.$$

实际上，就是$(\mathbf{I}_5, +)$同构于$\mathbf{S}_5$中$(1\ 2\ 3\ 4\ 5)$生成的循环群. ▌

例题 4 在凯莱定理的证明中，元素所导出的左乘变换起了很大作用，我们是否可以对应的使用元素导出的右乘变换同样地证明凯莱定理呢？

证明 先检查一下命题 2,3,4 对右乘变换是否照样成立.

设 G 是个群，a 是 G 中固定元素，通过 a 可以得到 G 上一个变换 ρ_a，

$$\rho_a(x) = xa, \quad 对每个\ x \in G.$$

则 ρ_a 是 G 上可逆变换. 证明的方法与命题 2 完全一样.

进一步，设 G 中元素所有右乘变换构成的集合为 R，则 R 是 $I(G)$的子群. 关键是，对任意 λ_a, ρ_b，由于对每个 $x \in G$ 必有

$$(\rho_a \circ \rho_b)(x) = \rho_a(\rho_b(x)) = \rho_a(xb) = (xb)a = x(ba),$$

即 $\rho_a \circ \rho_b = \rho_{ba} \in R$.

所以,有相应于命题 3 的结果.

但是,从上式也可以看出,在一般的非交换群中,规定 G 到 R 的映射 f,

$$f(a) = \rho_a, \quad a \in G,$$

则只会得到 f 是双射. 对任意 $a, b \in G$,有

$$f(ab) = \rho_{ab} = \rho_b \circ \rho_a = f(b)f(a),$$

而不一定永远有

$$f(ab) = f(a)f(b).$$

所以,我们不能照搬命题 4. 但是,可以有这样的结论:令 g 为 G 到 R 的映射

$$g(a) = \rho_{a^{-1}}, \quad a \in G.$$

关于 g 是 G 到 R 的双射,读者可自证之. 现在,任取 $a, b \in G$,证明

$$g(ab) = g(a)g(b).$$

因为等式之两端均为 G 上变换,我们只要证明,它们作用在 G 的每一个元素 x 上效果都相同. 事实上,有

$$\begin{aligned}
& g(ab)(x) \\
&= \rho_{(ab)^{-1}}(x) && (g\text{ 的定义}) \\
&= x(ab)^{-1} && (\rho\text{ 的定义}) \\
&= xb^{-1}a^{-1} && ((ab)^{-1} = b^{-1}a^{-1}) \\
&= (\rho_{b^{-1}}(x))a^{-1} && (\rho\text{ 的定义}) \\
&= \rho_{a^{-1}}[\rho_{b^{-1}}(x)] && (\rho\text{ 的定义}) \\
&= (\rho_{a^{-1}} \circ \rho_{b^{-1}})(x) && (\text{映射合成的定义}) \\
&= [g(a)g(b)](x) && (g\text{ 的定义})
\end{aligned}$$

这说明,从右侧出发同样可以证明凯莱定理. ▌

关于群 G 上的可逆变换,还有一类比较重要的变换今后要经

常遇到(见习题一题 1).

命题 5 设 G 是个群，a 是 G 的一个固定元素，通过 a 可导出一个 G 到 G 的映射 γ,

$$\gamma_a(x)=axa^{-1},\ x\in G.$$

那么 γ_a 必为 G 到 G 的同构映射.

证明 对任意 $a\in G$,必有

$$\gamma_a=\lambda_a\circ\rho_{a^{-1}}=\rho_{a^{-1}}\circ\lambda_a,$$

其中 λ_a 是 a 导出的左乘变换，ρ_a 是 a 导出的右乘变换. 这只要看，对每个 $x\in G$,

$$\gamma_a(x)=axa^{-1}=a(\rho_{a^{-1}}(x))=(\lambda_a\circ\rho_{a^{-1}})(x),$$

即可.

由于每个左乘变换和每个右乘变换都是可逆的，所以它们的乘积亦可逆，γ_a 为双射.

进一步，对任意 $x,y\in G$,

$$\gamma_a(xy)=a(xy)a^{-1}=(axa^{-1})(aya^{-1})=\gamma_a(x)\gamma_a(y),$$

所以，γ_a 是同构映射. ▌

定义 2 设 G 是个群. G 的元素 a 所导出的映射 γ_a 称为 a 导出的**内自同构**.

在第二章 §3 关于置换群的讨论中，我们知道，对有限集 S 的任意一个子集 T,若 G 是 S 上的一个置换群，则

$$G^T=\{P\in G\mid P(T)\subseteq T\}$$

是 G 的一个子群.

一般地，若 f 是集合 A 到 A 本身的一个映射，T 是 A 的子集，且

$$f(T)\subseteq T,$$

则说 T 是 f 的一个**不变子集**. 此时 f 在 T 上的限制 $f1_T$ 就是 T 到 T 本身的一个映射. 这个概念广泛应用于数学的各个分支，特别是线性代数学、拓扑学、泛函分析等等.

定义 3 设 G 是个群，H 是 G 的一个子群，如果 H 在每个内自同构映射之下都不变，即对任意 $a\in G$，任意 $h\in H$，都有

$$aha^{-1}\in H,$$

则说 H 是 G 的**不变子群**或**正规子群**，并记成 $H\lhd G$.

例 3 对任意群 G，都有 $G\lhd G$，$\{e\}\lhd G$.

事实上，对任意 $a\in G$，由

$$aea^{-1}=e\in\{e\},$$

即知 $\{e\}$ 是 G 的不变子群.

G 和 $\{e\}$ 称为 G 的**平凡的不变子群**.

例 4 当群 G 为交换群时，它的每个子群 H 都是不变的.

这是因为，对任意 $a\in G$，$h\in H$，$aha^{-1}=aa^{-1}h=h\in H$.

例 5 在 3 阶对称群 $\mathbf{S}_3$ 中，子群

$$H=\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$$

是 $\mathbf{S}_3$ 的不变子群.

我们只要验证 a 为 $(1\ 2)$，$(1\ 3)$，$(2\ 3)$，h 为 $(1\ 2\ 3)$ 和 $(1\ 3\ 2)$ 的情形，其他情形 $aha^{-1}\in H$ 是十分明显的. 计算

$$\begin{aligned}(1\ 2)(1\ 2\ 3)(1\ 2)^{-1}&=(1\ 2)(1\ 2\ 3)(1\ 2)\\&=(1\ 3\ 2)\in H,\\(1\ 3)(1\ 2\ 3)(1\ 3)&=(1\ 3\ 2)\in H,\\(2\ 3)(1\ 2\ 3)(2\ 3)&=(1\ 3\ 2)\in H,\\(1\ 2)(1\ 3\ 2)(1\ 2)&=(1\ 2\ 3)\in H,\\(1\ 3)(1\ 3\ 2)(1\ 3)&=(1\ 2\ 3)\in H,\\(2\ 3)(1\ 3\ 2)(1\ 3)&=(1\ 2\ 3)\in H.\end{aligned}$$

故有 $H\lhd G=\mathbf{S}_3$.

事实上，此例是下面例题的特殊情形.

例 6 在对称群 $\mathbf{S}_3$ 中，子群

$$H=\{(1),(1\ 2)\}$$

不是不变子群. 因为 $(1\ 2)\in H$，但

$$(1\ 2\ 3)(1\ 2)(1\ 2\ 3)^{-1}=(1\ 2\ 3)(1\ 2)(1\ 3\ 2)$$

$$=(2\ 3)\notin H.$$

命题 6 设 H 是群 G 的子群. 那么 H 是 G 的不变子群的充分必要条件是对任意 $g\in G$, $gH=Hg$.

证明 如果 H 是 G 的不变子群,我们来证明 $gH\subseteq Hg$,且

$$Hg\subseteq gH.$$

任取 $y\in gH$,即 $y=gx$, $x\in H$. 由于 H 是不变子群,必有

$$gxg^{-1}\in H.$$

令 $gxg^{-1}=z\in H$. 于是得到

$$gx=zg\in Hg,$$

这说明 $gH\subseteq Hg$.

同样,任取 $v\in Hg$,设 $v=ug$, $u\in H$. 由于 H 是不变子群,应有

$$(g^{-1})u(g^{-1})^{-1}=g^{-1}ug\in H.$$

设 $g^{-1}ug=w$,则得到

$$ug=gw\in gH.$$

也就是 $Hg\subseteq gH$. 所以 $gH=Hg$.

反过来,如果对任意 $g\in G$,它的左陪集 gH 恒与其右陪集 Hg 相等,那么对任意 $a\in G$ 和任意 $h\in H$,由于

$$ah\in aH=Ha$$

知道必有 $x\in H$ 使得

$$ah=xa\in Ha;$$

从而

$$aha^{-1}=x\in H.$$

所以,H 是 G 的不变子群. ∎

例题 5 设 H 是群 G 的子群,G 的阶数有限,且 $|G|=2|H|$. 则 H 必为 G 的不变子群.

证明 在第二章 §5 的例题中,我们已经证明了,此时 G 对 H 只有两个陪集,每个左陪集都是右陪集. 即对任意 $a\in G$,都有

$$aH=Ha.$$ ∎

例题 6 设 A, B 是群. 那么 $\{e_A\}\otimes B$ 是 $A\otimes B$ 的不变子群；同样，$A\otimes\{e_B\}$ 也是 $A\otimes B$ 的不变子群.

证明 对任意 $(a,b)\in A\times B$ 及任意 $(e_A, x)\in\{e_A\}\times B$，有

$$
\begin{aligned}
&(a,b)(e,x)(a,b)^{-1} \\
&\quad=(a,b)(e,x)(a^{-1},b^{-1}) &&(\text{外直积中求逆元})\\
&\quad=(aea^{-1},bxb^{-1}) &&(\text{外直积的乘法})\\
&\quad\in\{e\}\times B. &&(aea^{-1}=e)
\end{aligned}
$$

所以，$\{e\}\times B$ 是 $A\otimes B$ 的不变子群. ▌

例题 7 设 G 是个群，K 是其子群，N 是 G 的不变子群. 则 $KN=NK$ 且 KN 也是 G 的子群.

证明 注意，$KN=\{x\in G\mid x=kh,\ k\in K,\ h\in H\}$. 由于 $N\triangleleft G$，故任取 $x\in KN$，

$$x=kh,\ k\in K,\ h\in N.$$

那么，都应有 $kh\in kN=Nk\subseteq NK$. 这说明 $KN\subseteq NK$. 对称地，还有 $NK\subseteq KN$. 所以，有 $NK=KN$.

进一步，由于 $e_G\in N$，$e_G\in K$，从而有 $e_G=e_Ge_G\in NK$.

再任取 $h_1,h_2\in N$ 和 $k_1,k_2\in K$. 由于

$$k_1h_2\in KN=NK,$$

则必有 $k_3\in K$，$h_3\in N$ 使得 $k_1h_2=h_3k_3$. 于是

$$(h_1k_1)(h_2k_2)=h_1(h_3k_3)k_2=(h_1h_3)(k_3k_2)\in NK.$$

同时，对任意 $k\in K, h\in N$，有

$$(hk)^{-1}=k^{-1}h^{-1}\in KN=NK,$$

从而 NK 中元素的逆元仍在 NK 中.

所以，NK 是 G 的子群. ▌

命题 7 设 N 和 H 都是群 G 的不变子群，则 NH 也是 G 的不变子群.

证明 据命题 6 已知 NH 是 G 的子群. 并且，对任意 $n\in N$，$h\in H$ 和任意 $a\in G$ 有

$$a(nh)a^{-1}=(ana^{-1})(aha^{-1}).$$

但是 N 和 H 都是 G 的不变子群，从而

$$ana^{-1}\in N,\ aha^{-1}\in H;$$

进而有 $a(nh)a^{-1}\in NH$. ▍

命题 8 设 G 是个群，N_α 都是 G 的不变子群，$\alpha\in M$. 那么 $N=\bigcap_{\alpha\in M}N_\alpha$ 也是 G 的不变子群.

证明 我们已经知道 N 是 G 的子群，而对任意 $a\in G$ 及任意 $h\in N$，由于 $h\in N_\alpha$，$\alpha\in M$，同时 N_α 为 G 的不变子群，故有

$$aha^{-1}\in N_\alpha,\quad 对所有\ \alpha\in M.$$

于是，$aNa^{-1}\subseteq\bigcap_{\alpha\in M}N_\alpha=N$. ▍

为帮助读者加深对命题 7 和 8 的理解，我们再举几个例子.

例题 8 K,H 都是群 G 的子群不能保障 KH 必为 G 的子群.

如，在对称群 $\mathbf{S}_3$ 中，取

$$K=\{(1),(1\ 2)\},\quad H=\{(1),(1\ 3)\},$$

它们都是 $\mathbf{S}_3$ 的子群，但

$$KH=\{(1),(1\ 2),(1\ 3),(1\ 3\ 2)\}$$

不是 $\mathbf{S}_3$ 的子群. $\mathbf{S}_3$ 是 6 阶群. 不会有 4 阶的子群. ▍

例题 9 设 G 是所有 n 阶非奇异的实矩阵在矩阵乘法之下作成的群，H 是其中行列式值为 1 的矩阵形成的子群，那么 H 是 G 的不变子群.

证明 任取 $A\in G$，$B\in H$. 由于 A 非奇异，知道必然有 $|A|\neq 0$. 而 $|B|=1$，所以

$$|ABA^{-1}|=|A||B||A|^{-1}=|A||A|^{-1}=1,$$

即 $ABA^{-1}\in H$. ▍

我们知道，如果 H 是 G 的子群，K 是 H 的子群，则 K 也是 G 的子群.

但是，如果 H 是 G 的子群，K 是 H 的不变子群，那么 K 未必

是G的不变子群.因为K是H的不变子群的充要条件是对任意$k\in K$和任意$h\in H$,有

$$hkh^{-1}\in H;$$

这个条件不能保障对任意$k\in K$和任意$g\in G$有$ghg^{-1}\in H$.

最简单的反例,如果H是G的子群而不是不变子群,那么H是H本身的不变子群,但H不是G的不变子群.

进一步问,不变子群的不变子群是否为原群的不变子群,可用下例说明之.

用H代表4阶对称群$\mathbf{S}_4$中所有偶置换作成的子群.由于$|\mathbf{S}_4|=2|H|$,知H是$\mathbf{S}_4$的不变子群.

令

$$K=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\},$$

则K是H的子群.这是因为,K中4个置换都是偶置换,而它们之间的乘法表如下

·	(1)	(1 2)(3 4)	(1 3)(2 4)	(1 4)(2 3)
(1)	(1)	(1 2)(3 4)	(1 3)(2 4)	(1 4)(2 3)
(1 2)(3 4)	(1 2)(4 3)	(1)	(1 4)(2 3)	(1 3)(2 4)
(1 3)(2 4)	(1 3)(2 4)	(1 4)(2 3)	(1)	(1 2)(3 4)
(1 4)(2 3)	(1 4)(2 3)	(1 3)(2 4)	(1 2)(3 4)	(1)

它的特点是每个元素的阶数为2,除单位置换外,任意2个不同的置换乘积等于另外一个.这是一个颇有典型性的四元群(见习题一之题7).

对任意$\pi\in H$,设

$$\pi=\begin{pmatrix}1 & 2 & 3 & 4\\ i & j & k & l\end{pmatrix},\quad \pi^{-1}=\begin{pmatrix}i & j & k & l\\ 1 & 2 & 3 & 4\end{pmatrix},$$

其中i,j,k,l是数字1,2,3,4的一个排列.计算$\pi(1\ 2)(3\ 4)\pi^{-1}$,应有

$$\begin{array}{cccc} i & j & k & l \\ 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ j & i & l & k \end{array} \qquad \begin{array}{c} \pi^{-1} \\ (1\ 2)(4\ 3) \\ \pi \end{array}$$

故 $\pi(1\ 2)(3\ 4)\pi^{-1}=(i,j)(k,l)\in K$.同理,$\pi(1\ 3)(2\ 4)\pi^{-1}$和 $\pi(1\ 4)(2\ 3)\pi^{-1}$也在 K 中.这说明 K 是H 的不变子群.

再进一步,$L=\{(1),(1\ 2)(3\ 4)\}$是 K 的不变子群,因为 K 是交换群,每个子群都是其不变子群.

但,L 不是群H 的不变子群.因为$(1\ 2\ 3)$是偶置换,即$(1\ 2\ 3)\in H$,但

$$\begin{aligned}(1\ 2\ 3)(1\ 2)(3\ 4)(1\ 2\ 3)^{-1}&\\&=(1\ 2\ 3)(1\ 2)(3\ 4)(1\ 3\ 2)\\&=(1\ 4)(3\ 2)\notin L.\end{aligned}$$

例题 10 在所有复的可逆 2 阶矩阵构成的乘法群中,矩阵

$$I=\begin{pmatrix}1&0\\0&1\end{pmatrix},\ A=\begin{pmatrix}\mathrm{i}&0\\0&-\mathrm{i}\end{pmatrix},\ B=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\ C=\begin{pmatrix}0&\mathrm{i}\\\mathrm{i}&0\end{pmatrix}$$

和

$$-I=\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\ -A=\begin{pmatrix}-\mathrm{i}&0\\0&\mathrm{i}\end{pmatrix},\ -B=\begin{pmatrix}0&-1\\1&0\end{pmatrix},$$

$$C=\begin{pmatrix}0&-\mathrm{i}\\-\mathrm{i}&0\end{pmatrix}$$

作成一个子群(第二章§2 习题).证明:该群的每个子群都是其不变子群.

证明 注意此群 G 的运算特点,

$$A^2=-I,\ B^2=-I,\ C^2=-I.$$

又该群之阶数为 8,其非平凡子群之阶数只能为 2 或 4.

子群若含 A 或$-A$ 则必含$A^2=-I$ 或$(-A)^2=-I$,其阶数必大于 2,故它的 2 阶子群不能含$\pm A$,$\pm B$ 或$\pm C$,只能是

$$H=\{I,-I\}.$$

而

$$K=\{I,-I,A,-A\},\quad L=\{I,-I,B,-B\},$$

$$J=\{I,-I,C,-C\}$$

都是该群之子群. 同时,子群含 A 和 B 时,由 $AB=C$,知必含 C. 从而阶数大于 4. 同理,4 阶子解不能同时含 B 和 C、B 和 $-C$、A 和 $-C$ 等等. 即只能有上述 3 个 4 阶子群.

因为 I 和 $-I$ 与 G 的每个元素的乘积均可交换顺序,H 显然是 G 的不变子群.

注意 A,B,C 三个元素中任意两个的乘积必为另一元或其负矩阵. 这样,很容易算出

$$BAB^{-1}=(-C)(-B)=CB=-A,$$

$$CAC^{-1}=B(-C)=-BC=-A,$$

所以,$\{I,-I,A,-A\}$为 G 的不变子群. ▌

例题 11 设 G 是个群. 那么,G 中所有形如

$$a_1b_1a_1^{-1}b_1^{-1}a_2b_2a_2^{-1}b_2^{-1}\cdots a_nb_na_n^{-1}b_n^{-1},\quad n=1,2,\cdots$$

的元素的集合 X 是 G 的一个不变子群.

证明 用 e 代表 G 之恒等元,则 $e=eee^{-1}e^{-1}\in X$.

对任意$a_1b_1a_1^{-1}b_1^{-1}\cdots a_nb_na_n^{-1}b_n^{-1}$, $c_1d_1c_1^{-1}d_1^{-1}\cdots c_md_mc_m^{-1}d_m^{-1}\in X$,它们的乘积

$$a_1b_1a_1^{-1}b_1^{-1}\cdots a_nb_na_n^{-1}b_n^{-1}c_1d_1c_1^{-1}d_1^{-1}\cdots c_md_mc_m^{-1}d_m^{-1}$$

仍有所述形式,亦属于 X.

对任意 $a_1b_1a_1^{-1}b_1^{-1}\cdots a_nb_na_n^{-1}b_n^{-1}\in X$,它的逆元

$$b_na_nb_n^{-1}a_n^{-1}\cdots b_1a_1b_1^{-1}a_1^{-1}$$

仍有相同形式,亦属于 X.

所以,X 是 G 的子群.

对任意 $a\in G$ 及任意$a_1b_1a_1^{-1}b_1^{-1}\cdots a_nb_na^{-1}b_n^{-1}\in X$,则

$$\begin{aligned}&a\,(a_1b_1a_1^{-1}b_1^{-1}\cdots a_nb_na_n^{-1}b_n^{-1})a^{-1}\\&\quad=(aa_1a^{-1})(ab_1a^{-1})(aa_1a^{-1})^{-1}(ab_1a^{-1})^{-1}\cdots\\&\qquad(aa_na^{-1})(ab_na^{-1})(aa_na^{-1})^{-1}(ab_na^{-1})^{-1}\end{aligned}$$

仍在 X 中.故 X 是 G 的不变子群. ▌

定义 4 设 G 是个群, G 中由所求换位子元素

$$aba^{-1}b^{-1}, \quad a,b\in G$$

生成的子群(即所有形如

$$a_1b_1a_1^{-1}b_1^{-1}a_2b_2a_2^{-1}b_2^{-1}\cdots a_nb_na_n^{-1}b_n^{-1}, \quad n=1,2,\cdots$$

的集合)称为是 G 的**换位子群**.

定义 5 若群不含非平凡的不变子群则称为**单群**.

单群概念说起来简单,但单群的结构并不简简单单地一致,即使是有限单群也分成很多复杂的类型.

习 题 二

1. 给出 $\mathbf{I}_5$ 加群的所有自同构.

2. 所有实的 n 元列所构成的加群$(\mathbf{R}^n,+)$中,取定一个 n 阶可逆实矩阵 A,对任意$(a_1,\cdots,a_n)\in\mathbf{R}^n$,即 $a_1,\cdots,a_n\in\mathbf{R}$,令其对应$(a_1,\cdots,a_n)A$.则

$$f:(a_1,\cdots,a_n)\to(a_1,\cdots,a_n)A$$

是$(\mathbf{R}^n,+)$到$(\mathbf{R}^n,+)$的一个自同构.

3. 设 H 是群 G 的不变子群,且 H 的阶数等于 2.证明:$H\subseteq Z$, Z 是 G 的中心.

4. 用 λ_a 代表群 G 中元素 a 导出的左乘变换,ρ_b 代表元素 b 导出的右乘变换.证明:$\rho_b\lambda_a=\lambda_a\rho_b$.

5*. 设 G 是个群,H 和 K 都是 G 的不变子群,且 $H\cap K=\{e\}$.那么,对任意 $x\in H$, $y\in K$,恒有 $xy=yx$.

6. 设 $G=\{e,a,b,c\}$是克莱因四元群,其乘法表是

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

证明:G 的所有自同构组成的群 Aut(G)同构于对称群 S_3.

§3 群的同态

两个群同构时，尤如一个是另一个的复制品，其大小和结构完全相同.

比同构更一般的概念是同态，尤如从照片上反映人物特性，地球仪反映地球表面，沙盘模拟战场，等等，后者表现前者在一定要求下的基本属性，不要求一模一样.

同态乃是一个群到另一个群的映射，不要求是双射，这样，映射的像通常比原来的群要来得"小"些.

同态概念同样使用于环论、模论等几乎所有代数学领域，是代数学的最重要概念之一.

定义 1 设$(G,\circ)$是个群，$(H,\#)$也是个群，那么，G 到 H 的映射 f 称为是 G 到 H 的**同态映射**，如果对任意 $a,b\in G$ 都有

$$f(a\circ b)=f(a)\# f(b).$$

粗略地说，同态就是保运算的映射.

例 1 所有的同构映射都是同态映射.

例 2 整数加法群$(\mathbf{I},+)$到整数加法群自己$(\mathbf{I},+)$的映射 f,

$$f(m)=2m,\quad 每个\ m\in\mathbf{I},$$

是个同态映射

例 3 任取一个实数 a，由它导出一个从实数加群$(\mathbf{R},+)$到$(\mathbf{R},+)$的映射 ρ_a，

$$\rho_a(r)=ar,\quad 每个\ r\in\mathbf{R}.$$

由于对任意 $r,s\in\mathbf{R}$ 都有

$$\begin{aligned}
&\rho_a(r+s)\\
&\quad=a(r+s) && (\rho_a\text{ 的定义})\\
&\quad=ar+as && (\text{实数加乘的分配律})\\
&\quad=\rho_a(r)+\rho_a(s), && (\rho_a\text{ 的定义})
\end{aligned}$$

故 ρ_a 为$(\mathbf{R},+)$到$(\mathbf{R},+)$的同态映射.

例 4* 设(G,Δ),$(H,\circ)$是群,$G\otimes H$ 是它们的处直积.规定,任意$(g,h)\in G\times H$ 对应G 中元g.则得 $G\otimes H$ 到G 的映射,记为 π_1,即

$$\pi_1((g,h))=g,\quad 每个(g,h)\in\times H,$$

则 π_1 是 $G\otimes H$ 到G 的同态.

事实上,对任意(g^1,h_1),$(g_2,h_2)\in G\times H$,都有

$$\begin{aligned}
&\pi_1((g_1,h_1)\otimes(g_2,h_2))\\
&\quad=\pi_1((g_1\Delta g_2,h_1\circ h_2)) && (\otimes\text{的定义})\\
&\quad=g_1\Delta g_2 && (\pi_1\text{ 的定义})\\
&\quad=\pi_1((g_1,h_1)\Delta\pi_1(g_2,h_2)). && (\pi_1\text{ 的定义})
\end{aligned}$$

例 5 设 G 是所有实的 n 阶非奇异矩阵作成的乘法群.规定,每个矩阵 $A\in G$,对应它的行列式$|A|$,则得 G 到非零实数乘法群的一个映射

$$f(A)=|A|,\quad A\in G.$$

这是个同态映射,因为线性代数学中已经证明,对任意 $A,B\in G$,恒有

$$f(AB)=|AB|=|A|\,|B|=f(A)f(B).$$

例 6 设 $\mathbf{S}_n$ 是 n 阶对称群,规定 $\mathbf{S}_n$ 到二元群$\{e,a\}$的映射 f,对任意 $A\in\mathbf{S}_n$,

$$f(A)=\begin{cases}e, & 如果 A 为偶置换,\\ a, & 如果 A 为奇置换.\end{cases}$$

则 f 是个同态映射.

这是因为,我们证明过,任意两个 n 阶置换A,B,如果它们奇偶性相同,则 AB 为偶置换;如果它们的奇偶性相反,则 AB 为奇置换.

置换 A,B 之奇偶性相同,即 $f(A)$和 $f(B)$同时为 e 或同时

为a,则 AB 为偶置换,即 $f(AB)$为 e. 由于 $aa=ee=e$,所以

$$f(A)f(B)=f(AB).$$

置换 A,B 之奇偶性相反,即 $f(A)$和 $f(B)$中一个为 a,一个为 e,则 AB 为奇置换,即 $f(AB)=a$. 由于 $ae=ea=a$,故

$$f(A)f(B)=f(AB).$$

总之,不论何种情形,恒有 $f(A)f(B)=f(AB)$. 故,f 是同态映射.

例 7 对一固定的正整数 n,我们来建立群$(\mathbf{I},+)$到群$(\mathbf{I}_n,+)$的一个同态映射.

对于$(\mathbf{I}_n,+)$的具体运算规律,读者可再复习一下第一章 §6 例 9.

首先,建立映射 $f:\mathbf{I}\to\mathbf{I}_n$. 作法是,对任意 $m\in\mathbf{I}$,作除法,得

$$m=qn+r,\quad 0\leqslant r<n,$$

r 是由 m 唯一确定的. 而 r 唯一确定 r^*,令

$$f(m)=r^*,$$

即得 $\mathbf{I}$ 到 $\mathbf{I}_n$ 的映射.

对任意 $m_1,m_2\in\mathbf{I}$,设

$$\begin{aligned}m_1&=nq_1+r_1,\quad 0\leqslant r_1<n,\\ m_2&=nq_2+r_2,\quad 0\leqslant r_2<n,\\ r_1+r_2&=nq+r,\quad 0\leqslant r<n.\end{aligned}\tag{1}$$

由 f 的定义,知 $f(m_1)=r_1,f(m_2)=r_2$. 由群$(\mathbf{I}_n,+)$中加法定义知 $r_1^*+r_2^*=r^*$,所以,有 $f(m_1)+f(m_2)=r^*$.

另一方面,把(1)中 3 个等式连起来,得

$$m_1+m_2=n(q_1+q_2+q)+r,\quad 0\leqslant r<n.$$

故由 f 的定义知

$$f(m_1+m_2)=r^*.$$

所以,$f(m_1+m_2)=f(m_1)+f(m_2)$.

f 是 $\mathbf{I}$ 到 $\mathbf{I}_n$ 的同态映射.

例题 1 设 f 是$(\mathbf{I},+)$到$(\mathbf{I},+)$的映射,

$$f(x)=x^2,\quad x\in\mathbf{I}.$$

说明 f 不是 $\mathbf{I}$ 到 $\mathbf{I}$ 的同态映射.

证明 取 $2,-2\in\mathbf{I}$,则

$$f(2)=4,\quad f(-2)=4.$$

但 $f(2+(-2))=f(0)=0$,从而

$$f(2+(-2))\neq f(2)+f(-2).$$

f 不是$(\mathbf{I},+)$到$(\mathbf{I},+)$的同态映射. ▌

命题 1 设 f 是群$(G,\circ)$到$(H,\#)$的同态映射.那么

$$f(e_G)=e$$

证明 对任意 $h\in H$,有

$$\begin{aligned}
&h\# f(e_G)\\
&\quad=h\# f(e_G\circ e_G) && (e_G\circ e_G=e_G)\\
&\quad=h\#[f(e_G)\# f(e_G)] && (f\text{ 是同态映射})\\
&\quad=[h\# f(e_G)]\# f(e_G). && (H\text{ 中有结合律})
\end{aligned}$$

由于群 H 中有消去律,故

$$h=h\# f(e_G),$$

再由群 H 中恒等元的唯一性,即知 $f(e_G)$是 H 的恒等元,即

$$f(e_G)=e_H.$$ ▌

命题 2 设 f 是群$(G,\circ)$到群$(H,\#)$的同态映射,那么,对 G 中任意元素 g,元素 $f(g)$在 H 中的逆元素恰为$f(g^{-1})$,即

$$f(g)^{-1}=f(g^{-1}).$$

证明 由于 $f(e_G)=e_H$,且

$$f(g)\# f(g^{-1})=f(g\circ g^{-1})=f(e_G)=e_H,$$

故 $f(g^{-1})$是 $f(g)$的逆元素,$f(g^{-1})=f(g)^{-1}$. ▌

命题 3 设 f 是群$(G,\circ)$到群$(H,\#)$的同态映射,那么 H 中

恒等元 e_H 的原像

$$K=f^{-1}(e_H)=\{g\in G\mid f(g)=e_H\}$$

是 G 的不变子群.

证明 首先,由命题 1 知,$f(e_G)=e_H$,故 $e_G\in K$.

其次,若 $a,b\in K$,即 $f(a)=e_H$, $f(b)=e_H$,则

$$f(a\circ b)=f(a)\# f(b)=e_H\# e_H=e_H,$$

即 $a\circ b\in K$.

再次,若 $a\in K$,即 $f(a)=e_H$,则

$$f(a^{-1})=f(a)^{-1}=e_H^{-1}=e_H,$$

即 $a^{-1}\in K$.

这说明 K 是 G 的一个子群.

最后,任取 $g\in G$, $a\in K$,都有

$$\begin{aligned}
&f(g\circ a\circ g^{-1})\\
&\quad=f(g)\# f(a)\# f(g^{-1}) &&(f\text{ 是同态映射})\\
&\quad=f(g)\# e_H\# f(g^{-1}) &&(a\in K,\ f(a)=e_H)\\
&\quad=f(g)\# f(g^{-1}) &&(e_H\text{ 是 }H\text{ 的恒等元})\\
&\quad=f(g)\# f(g)^{-1} &&(f(g^{-1})\text{是 }f(g)\text{的逆})\\
&\quad=e_H.
\end{aligned}$$

即 $g\circ a\circ g^{-1}\in K$.

所以,K 是 G 的不变子群. ▌

定义 2 设 f 是群$(G,\circ)$到$(H,\#)$的一个同态映射,那么称 e_H 的原像 $f^{-1}(e_H)$为映射 f 的核,记为 $\mathrm{Ker}(f)$.

例 2 中,$\mathbf{I}$ 的恒等元是 0,若 $f(m)=2m=0$,则 $m=0$,故

$$\mathrm{Ker}(f)=\{0\}.$$

例 4 中,G 的恒等元是 e_G,若 $\pi_1((g,h))=g=e_G$,则$(g,h)=(e_G,h)$,也就是说

$$\mathrm{Ker}(f)=H'=\{(g,h)\in G\otimes H\mid g=e_G\},$$

其中 H' 等的性质读者可复习第二章§6命题3.

例5中,实数乘法群的恒等元是数1,故

$$\operatorname{Ker}(f)=\{A\in G \mid |A|=1\},$$

即所有行列式为1的矩阵的集合 H(见§2的例题)恰为 f 的核.

例6中,二元群 $\{e,a\}$ 之恒等元为 e, e 的原像乃是全体偶置换所构成的集合.

例7中,$\mathbf{I}_n$ 的零元是 0^*, $f(m)=0^*$ 当而且仅当 $m=nq$,即 n 整除 m,故 $\operatorname{Ker}f=f^{-1}(0^*)=\{\cdots,-n,0,n,\cdots\}$.

命题4 如果 f 是群$(G,\circ)$到群$(H,\#)$的同态映射,g 是群$(H,\#)$到群$(K,*)$的同态映射,则 gf 是群$(G,\circ)$到群$(K,*)$的一个同态映射.

证明 要证明 G 到 K 的映射 gf 是群的同态映射,我们任取 $a,b\in G$,则有

$$
\begin{aligned}
&(gf)(a\circ b)\\
&=g(f(a\circ b)) && \text{(映射合成的定义)}\\
&=g(f(a)\# f(b)) && \text{(g 是同态映射)}\\
&=g(f(a))*g(f(b)) && \text{(g 是同态映射)}\\
&=(gf)(a)*(gf)(b). && \text{(映射合成的定义)}
\end{aligned}
$$

命题得证. ▌

对于群的同态映射 $f:G\to H, g:H\to K$ 和 $h:G\to K$,如果 $h=gf$,则映射的图形图3-1可交换.反过来,上面的图形恒意味着 f,g 都是群的同态,且 $h=gf$.

定理1 设 f 是群$(G,\circ)$到群$(H,\#)$的同态映射,g 是群$(H,\#)$到群$(K,*)$的同态映射.那么,有

$$\operatorname{Ker}(gf)=f^{-1}(\operatorname{Ker}(g)).$$

证明 首先要搞清楚,gf 是 G 到 K 的映射. $\operatorname{Ker}(gf)$ 是 G 的一个子集合. g 是 H 到 K 的映射, $\operatorname{Ker}(g)$ 是 H 的子集, $f^{-1}(\operatorname{Ker}(g))$ 是 G 的子集.我们要证明的是 G 中的子集的等式.

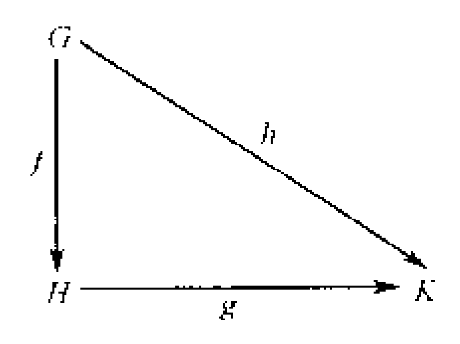


图 3-1

任取 $a \in G$，如果 $a \in \mathrm{Ker}(gf)$，即

$$(gf)(a)=e_K.$$

由于$(gf)(a)=g(f(a))=e_K$，知道$f(a)\in \mathrm{Ker}(g)$，故而得到

$$a \in f^{-1}(\mathrm{Ker}(g)).$$

反过来，如果 G 的元素 $a \in f^{-1}(\mathrm{Ker}(g))$，由原像的定义知 $f(a)\in \mathrm{Ker}(g)$，$f(a)$是 H 中的一个元素，它在 g 的核中，按核的定义，就是

$$g(f(a))=(gf)(a)=e_K,$$

从而 $a \in \mathrm{Ker}(gf)$.

所以，$\mathrm{Ker}(gf)\subseteq f^{-1}(\mathrm{Ker}(g))\subseteq \mathrm{Ker}(gf)$，也就是

$$\mathrm{Ker}(gf)=f^{-1}(\mathrm{Ker}(g)).$$ ∎

例题 2 设 f 是$(\mathbf{I},+)$到$(\mathbf{I}_8,+)$的映射，

$$f(m)=r^*, \quad m=8q+r,\ 0\leqslant r<8$$

(见例 7)；而 g 是$(\mathbf{I}_8,+)$到本身$(\mathbf{I}_8,+)$的映射，

$$g(i^*)=i^*+i^*, \quad i^*\in \mathbf{I}_8.$$

我们已经知道 f 是同态映射，g 是同态映射由读者自证. 求

$$\mathrm{Ker}(gf).$$

解 0^* 是 $\mathbf{I}_8$ 的恒等元，若 $i^*\in \mathbf{I}_8$ 使

$$g(i^*)=i^*+i^*=0^*,$$

按着 $\mathbf{I}_8$ 的加法规则，应有

$$i+i=8q, \quad 0\leqslant i<8.$$

也就是整数 $2i$ 应能被 8 整除，这样 i 只有 0 和 4. 即

$$\mathrm{Ker}(g)=\{0^*,4^*\}.$$

由定理 1，知 $\mathrm{Ker}(gf)=f^{-1}(\{0^*,4^*\})$，故

$$\mathrm{Ker}(gf)=\{\cdots,-8,-4,0,4,8,\cdots\}.$$ ▌

定理 2 设 f 是群 $(G,\circ)$ 到群 $(H,\#)$ 的同态映射，g 是 $(H,\#)$ 到群 $(K,*)$ 的同态映射. 那么 $\mathrm{Img}(gf)=g(\mathrm{Img}(f))$.

证明 由于 gf 是 G 到 K 的映射，故它的像 $\mathrm{Img}(gf)$ 是 K 的子集. 同时，$\mathrm{Img}(f)$ 是 H 的一个子集，它在 g 之下的像 $g(\mathrm{Img}(f))$ 也是 K 的一个子集. 我们要证明的是 K 中两个子集相等.

若 $k\in K$, $k\in\mathrm{Img}(gf)$，即有 $a\in G$，使

$$k=(gf)(a)=g(f(a)),$$

因为 $f(a)\in\mathrm{Img}(f)$，故

$$k\in g(\mathrm{Img}(f)).$$

这说明 $\mathrm{Img}(gf)\subseteq g(\mathrm{Img}(f))$.

反过来，若 $k\in K$, $k\in g(\mathrm{Img}(f))$，即有 $h\in\mathrm{Img}(f)$, $g(h)=k$. 由 $h\in\mathrm{Img}(f)$ 知道，必有 $a\in G$，使得 $h=f(a)$. 所以，

$$k=g(h)=g(f(a))=(gf)(a)\in\mathrm{Img}(gf).$$

这说明 $g(\mathrm{Img}(f))\subseteq\mathrm{Img}(gf)$.

所以，$g(\mathrm{Img}(f))=\mathrm{Img}(gf)$. ▌

命题 5 设 f 是群 $(G,\circ)$ 到群 $(H,\#)$ 的同态映射. 如果 A 是 G 的子群，则 $f(A)$ 是 H 的子群；如果 B 是 H 的子群，则 $f^{-1}(B)$ 是 G 的子群.

证明 由于 A 是 G 的子群，故 $e_G\in A$，从而 $f(e_G)=e_H\in f(A)$.

设 H 的元素 $x,y\in f(A)$，即有 $a,b\in A$ 使

$$x=f(a),\quad y=f(b),$$

从而 $x\#y=f(a)\#f(b)=f(a\circ b)$. 而 A 是 G 的子群，$a,b\in A$ 则 $a\circ b\in A$，故 $x\#y=f(a\circ b)\in f(A)$.

对任意 $x\in f(A)$, $x=f(a)$, $a\in A$，由于 A 是 G 的子群，故 $a^{-1}\in A$. 从而 $f(a)^{-1}=f(a^{-1})\in f(A)$.

$f(A)$ 是 H 的子群.

B 是 H 的子群，则 $e_H \in B$，而命题 1 表明 $f(e_G)=e_H$，故

$$e_G \in f^{-1}(B).$$

若 G 的元素 $a,b \in f^{-1}(B)$，即

$$f(a)\in B,\quad f(b)\in B,$$

由于 B 是 H 的子群，$f(a)\# f(b)\in B$，故

$$f(a\circ b)=f(a)\# f(b)\in B,$$

即 $a\circ b\in f^{-1}(B)$.

若 G 的元素 $a\in f^{-1}(B)$，即 $f(a)\in B$. 由于 B 是 H 的子群，必有 $f(a)^{-1}\in B$. 据命题 2，有 $f(a)^{-1}=f(a^{-1})\in B$，也就是 $a^{-1}\in f^{-1}(B)$.

所以，$f^{-1}(B)$是 G 的子群. ∎

可以看出，若 f 是群$(G,\circ)$到群$(H,\#)$的同态映射，则$f(G)$可以反映出 G 的一些性质. 如，G 有限则 $f(G)$有限；G 是可交换的则$f(G)$也是可交换的，G 是循环群则$f(G)$也是循环群，等等.

由于 H 中有些元素并不一定在f之下与G 的元素对应，很难要求整个群 H“保持”G 的某些代数性质.

定义 3 设$(G,\circ)$和$(H,\#)$都是群. 如果有$(G,\circ)$到$(H,\#)$的同态映射 f 是满的，则说群$(G,\circ)$同态于群$(H,\#)$，说$(H,\#)$是$(G,\circ)$的一个**同态像**.

例如，$(\mathbf{I},+)$同态于$(\mathbf{I}_8,+)$，也同态于$(\mathbf{I}_4,+)$. $\mathbf{I}\otimes\mathbf{I}$ 同态于 $\mathbf{I}$.

命题 6 设 f 是群$(G,\circ)$到群$(H,\#)$的满同态映射，A 是G 的不变子群，B 是H 的不变子群. 那么，$f(A)$是 H 的不变子群，$f^{-1}(B)$是 G 的不变子群.

证明 命题 5 已指明 $f(A)$是 H 的子群，$f^{-1}(B)$是 G 的子群.

对任意 $h\in H$ 及任意$f(a)\in f(A)$，$a\in A$，由于 f 是个满同态，必有 $g\in G$，$f(g)=h$. 从而

$$h\# f(a)\# h^{-1}=f(g)\# f(a)\# f(g^{-1})=f(g\circ a\circ g^{-1}),$$

但 A 是 G 的不变子群,必有 $g\circ a\circ g^{-1}\in A$,所以

$$h\# f(a)\# h^{-1}\in f(A),$$

$f(A)$是 H 的不变子群.

对任意 $g\in G$ 及任意 $a\in f^{-1}(B)$, $f(a)\in B$,我们有

$$f(g\circ a\circ g^{-1})=f(g)\# f(a)\# f(g)^{-1}.$$

由于 B 是 H 的不变子群,故 $f(g)\# f(a)\# f(g)^{-1}\in B$. 所以, $g\circ a\circ g^{-1}\in f^{-1}(B)$. 这说明 $f^{-1}(B)$是 G 的一个不变子群. ▌

定理 3 设 f 是群$(G,\circ)$到群$(H,\#)$的同态映射. 那么,f 是单射的充分必要条件是 $\mathrm{Ker}(f)=\{e_G\}$.

证明 如果 f 是单射,首先,有

$$f(e_G)=e_H$$

同时,对 G 中任意元 a,只要 $a\neq e_G$,则

$$f(a)\neq f(e_G),\quad f(a)\neq e_H.$$

所以,$\mathrm{Ker}(f)=f^{-1}(e_H)=\{e_G\}$.

反过来,如果 $\mathrm{Ker}(f)=\{e_G\}$,那么,只要 $a,b\in G$, $f(a)=f(b)$. 则必有

$$f(a)\# f(b)^{-1}=f(a\circ b^{-1})=e_H.$$

从而 $a\circ b^{-1}=e_G$, $a=b$. 这说明,f 是单射. ▌

把第一章§4 的命题 6 搬到这里,有

命题 7 设 f 是群 G 到群 H 的同态映射,B 为 H 的子群. 则

$$f(f^{-1}(B))=B\cap \mathrm{Img}(f).$$ ▌

同时,还有

命题 8 设 f 是群 G 到群 H 的同态映射,A 是 G 的子群. 则

$$f^{-1}(f(A))=A\,\mathrm{Ker}(f).$$

证明 因为 A 是 G 的子群,$\mathrm{Ker}(f)$是 G 的不变子群,上节例题中已证明,$A\,\mathrm{Ker}(f)=\mathrm{Ker}(f)\,A$ 是 G 的子群.

A 是 G 的子群,$f(A)$是 H 的子群,进而 $f^{-1}(f(A))$是 G 的

子群.

本命题要证明的是 G 中两个子群相等的问题.

如果 $g\in A\text{Ker}(f)$,设

$$g=ak,\quad a\in A,\ k\in \text{Ker}(f).$$

由 $k\in\text{Ker}(f)$知 $f(k)=e_H$,所以,

$$\begin{aligned}f(g)&=f(a\circ k)=f(a)\# f(k)\\&=f(a)\in f(A),\quad g\in f^{-1}(f(A)).\end{aligned}$$

这说明 $A\text{Ker}f\subseteq f^{-1}(f(A))$.

反过来,如果 $g\in f^{-1}(f(A))$,即 $f(g)\in f(A)$,则必有 $a\in A$,使 $f(g)=f(a)$.于是,在 H 中,

$$f(a)^{-1}\# f(g)=e_H.$$

而 f 是同态映射,$f(a^{-1}\circ g)=e_H$,也就是

$$a^{-1}\circ g\in\text{Ker}(f),\quad g\in a\text{Ker}(f)\subseteq A\text{Ker}(f),$$

这说明 $f^{-1}(f(A))\subseteq A\text{Ker}(f)$. ▌

例题 3 条件如例 5.用 E 代表 n 阶单位矩阵.求 G 的子群 $\{E,-E\}=H$ 所对应的 $f^{-1}(f(H))$.

解 由于 $\text{Ker}(f)=\{A\in G\,\big|\,|A|=1\}$,故

$$f^{-1}(f(H))=H\text{Ker}(f)=\{E,-E\}\text{Ker}(f).$$

而$(-E)\text{Ker}(f)=\{-A\,\big|\,|A|=1\}$,所以

$$H\text{Ker}(f)=\{\pm A\in G\,\big|\,|A|=1\}$$ ▌

从此例我们可以看到,G 的子群 H 只有两个元素,但它的像 $f(H)$的原像 $f^{-1}(f(H))$却比 H 要大的多,它包含了 H,也包含了 $\text{Ker}(f)$.

又如,在例 7 中取 $n=8$.看 $\mathbf{I}$ 的子群

$$A=\{\cdots,-6,0,6,\cdots\}.$$

先计算 $f(A)$.有

$$-6=-1\times 8+2,\quad f(-6)=2^*,$$

$$0=0\times 8+0,\qquad f(0)=0^*,$$

$$6=0\times 8+6,\qquad f(6)=6^*,$$
$$12=1\times 8+4,\qquad f(12)=4^*,$$
$$18=2\times 8+2,\qquad f(18)=2^*,\cdots.$$
即 $f(A)=\{0^*,2^*,4^*,6^*\}$,它是 I_8 的一个子群.

而 $f(A)$ 的原像 $f^{-1}(f(A))$,也就是 $0^*,2^*,4^*,6^*$ 四个元素的原像的并集,应为

$$\{\cdots,-6,2,10,\cdots\}\cup\{\cdots,-8,0,8,\cdots\},$$
$$\cup\{\cdots,-10,-2,6,\cdots\}\cup\{\cdots,-12,-4,4,\cdots\},$$

也就是

$$\{\cdots-6,-4,-2,0,2,4,6,\cdots\},$$

即全体偶数集作成的子群.

用命题 7 的公式算,它应当是 $A+\mathrm{Ker}(f)$,即

$$\begin{aligned}&\{\cdots,-6,0,6,\cdots\}+\{\cdots,-8,0,8,\cdots\}\\&=\{\cdots,(-6+0),(-12+8),(-8+6),0,(8+(-6)),\cdots\}\\&=\{\cdots,-6,-4,-2,0,2,4,\cdots\},\end{aligned}$$

也得到偶数集.

为了说话方便,我们把定理 3 的一个简单而有用的推论写成

命题 9 群 $(G,\circ)$ 到群 $(H,\#)$ 的满同态映射 f 是同构映射,当而且只当,$\mathrm{Ker}(f)=\{e_H\}$. ▌

例题 4 设 f 是群 $(G,\cdot)$ 到群 (H,Δ) 的同态映射,$a\in G$. 那么,对任意 $b\in G$, $b\in a\mathrm{Ker}(f)$ 的充分必要条件是 $f(b)=f(a)$.

证明 若 $f(b)=f(a)$,则

$$\begin{aligned}&f(a^{-1}\cdot b)\\&\quad=f(a^{-1})\Delta f(b)\qquad &&(f\text{ 是群同态映射})\\&\quad=f(a)^{-1}\Delta f(b)\qquad &&(\text{命题 }2)\\&\quad=e_H.\qquad &&(f(a)=f(b))\end{aligned}$$

这表明 $a^{-1}\cdot b\in\mathrm{Ker}(f)$,也就是 $b\in a\mathrm{Ker}(f)$.

反之,若 $b\in a\mathrm{Ker}(f)$,设 $x\in\mathrm{Ker}(f)$ 使 $b=a\cdot x$ 那么,应有

$$L:(x,y,z)\to(x+2y-z,2x+y-z,x-y-2z).$$

证明：L 是$(\mathbf{R}^3,+)$到$(\mathbf{R}^3,+)$的群同态并求出 L 的核.

4. 用 $\mathbf{C}^{\#}$ 代表非零复数的乘法群，用 $\mathbf{R}^{+}$ 代表正实数乘法群. 证明：

$$\sigma:a+ib\to\sqrt{a^2+b^2},\quad a,b\in\mathbf{R}$$

是 $\mathbf{C}^{\#}$ 到 $\mathbf{R}^{+}$ 的群同态，并给出 σ 的核.

5*. 看整数加群 $\mathbf{I}$ 的直积 $\mathbf{I}\times\mathbf{I}$ 到 $\mathbf{I}$ 的映射 σ，

$$\sigma:(m,n)\to 2m+n,\quad (m,n)\in\mathbf{I}\times\mathbf{I}.$$

证明：σ 是群同态映射，并求出 σ 的核.

§4 商 群

如果 N 是群 G 的一个不变子群. 那么，利用 N 可导出 G 的一个等价关系，$a\sim b$ 当而且仅当 $a^{-1}b\in N$，也就是 a,b 属于 N 的同一个左陪集.

由于 N 是不变子群，每一个左陪集就是一个右陪集，其陪集不区分左右，简称为**陪集**.

对于等价关系 $\sim$，我们可得到 G 的一个商集 $\bar{G}$，它的每个元素都是 N 的一个陪集，即 $\bar{G}=\{aN,bN,\cdots\}$.

在第二章§4 中，我们很自然地把整数集 $\mathbf{I}$ 对模 n 关系的商集

$$\bar{\mathbf{I}}=\{[a],[b],\cdots\}$$

定义成一个群$(\bar{\mathbf{I}},\boxplus)$. $\bar{\mathbf{I}}$ 的运算是由 $\mathbf{I}$ 的加法运算派生出来的.

现在，要讨论如何将任意群 G 对其不变子群 N 的商集定义成群. 这样得到的群即是所说的商群.

还要证明，群 G 的每个同态像必然同构于 G 的一个商群. 这样，从同构的观点看，只要把群的所有商群的结构研究清楚，那么它的所有同态像也就清楚了. 可见商群的概念是相当重要的.

本节要讲的同态基本定理实际上也是整个群的理论的基本定理，所以这一节在整个抽象代数学的教学中是特别值得重视的.

定理1 设 N 是群$(G,\circ)$的一个不变子群,G/N 代表G 对N 的所有陪集构成的集合,规定,任意,$aN,bN\in G/N$,对应 G/N 的元素$(a\circ b)N$,则得到 G/N 的一个运算,记为#,即

$$aN \# bN=(a\circ b)N.$$

进一步,$(G/N,\#)$是个群.

证明 首先来证明$(a\circ b)N$ 是由aN 和bN 唯一确定的,与陪集代表元的选择无关.这就是在第二章已经强调过的定义的合理性问题.

设 $a_1N=a_2N$, $b_1N=b_2N$.那么,必有 $u,v\in N$ 使得

$$a_1=a_2\circ u,\quad b_1=b_2\circ v.$$

从而 $a_1\circ b_1=a_2\circ(u\circ b_2)\circ v$.由于 N 是G 的不变子群,而

$$u\circ b_2\in Nb_2=b_2N,$$

又必有 $w\in N$,使 $u\circ b_2=b_2\circ w$.于是

$$a_1\circ b_1=a_2\circ(b_2\circ w)\circ v=(a_2\circ b_2)\circ x,$$

其中 $x=w\circ v\in N$,即 $a_1\circ b_1$ 和 $a_2\circ b_2$ 在同一个陪集中,

$$(a_1\circ b_1)N=(a_2\circ b_2)N.$$

即,无论代表元如何选取,得到的都是同一个陪集.

所以,规定(aN,bN)对应$(a\circ b)N$,记

$$aN\# bN=(a\circ b)N,$$

就得到 G/N 的一个运算#.

进一步,任取 G/N 的3个元素,设为 aN,bN,cN.则必有

$$\begin{aligned}
&(aN\# bN)\# cN\\
&=(a\circ b)N\# CN &&(\#\text{的定义})\\
&=((a\circ b)\circ c)N &&(\#\text{的定义})\\
&=(a\circ(b\circ c))N &&(\circ\text{满足结合律})\\
&=aN\#(b\circ c)N &&(\#\text{的定义})\\
&=aN\#(bN\# cN), &&(\#\text{的定义})
\end{aligned}$$

这说明，# 满足结合律.

又 $e_G N \in G/N$，且对任意陪集 aN，有

$$
\begin{aligned}
& e_G N \# aN \\
& = (e_G \circ a)N \qquad (\# \text{的定义}) \\
& = aN, \qquad (e_G \text{ 是 } G \text{ 的恒等元})
\end{aligned}
$$

即 G/N 有一个左恒等元 $e_G N = N$.

最后，对任意 $aN \in G/N$，看 $a^{-1}N \in G/N$，有

$$
\begin{aligned}
& a^{-1}N \# aN \\
& = (a^{-1} \circ a)N \qquad (\# \text{的定义}) \\
& = e_G N \qquad (a^{-1} \text{是 } a \text{ 的逆元}) \\
& = N, \qquad (e_G \text{ 在 } N \text{ 中})
\end{aligned}
$$

即 $a^{-1}N$ 是 aN 的左逆元.

所以，$(G/N, \#)$ 是个群. ▌

定义 1 设 N 是群 $(G, \circ)$ 的不变子群. 在商集 G/N 中规定

$$aN \# bN = (a \circ b)N; \quad aN, bN \in G/N.$$

则 $(G/N, \#)$ 作成群，称为群 $(G, \circ)$ 对不变子群 N 的商群.

这里，有两件事要引起读者注意.

第一，定理 1 的证明中，运算 # 的合理性的验证是必要的，不是说，对任意子群 N，对其左等价关系的商集 G/N，规定

$$aN * bN = (a \circ b)N$$

都有意义.

例如，设 G 是所有 2 阶非奇异的实矩阵在矩阵乘法下构成的群，且

$$H = \left\{ A \in G \mid A = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}, \ r \in \mathbf{R} \right\},$$

则 H 是 G 的一个子群.

用 G/H 代表 G 对 N 的所有左陪集构成的集合. 现规定，任意 aH，$bH \in G/H$ 对应 $(ab)H$，并且记 $aH \# bH = (ab)H$，…….

这是行不通的.因为

$$\bar{a}=\begin{pmatrix}1&0\\1&1\end{pmatrix}H=\left\{\begin{pmatrix}1&s\\1&s+1\end{pmatrix}\middle|s\in\mathbf{R}\right\},$$

$$\bar{b}=\begin{pmatrix}1&0\\-1&1\end{pmatrix}H=\left\{\begin{pmatrix}1&s\\-1&1-s\end{pmatrix}\middle|s\in\mathbf{R}\right\}.$$

容易看出

$$\begin{pmatrix}1&0\\1&1\end{pmatrix}\sim\begin{pmatrix}1&-1\\1&0\end{pmatrix},\quad \begin{pmatrix}1&0\\1&1\end{pmatrix}H=\begin{pmatrix}1&-1\\1&0\end{pmatrix}H,$$

$$\begin{pmatrix}1&0\\-1&1\end{pmatrix}\sim\begin{pmatrix}1&1\\-1&0\end{pmatrix},\quad \begin{pmatrix}1&0\\-1&1\end{pmatrix}H=\begin{pmatrix}1&1\\-1&0\end{pmatrix}H.$$

但是

$$\begin{pmatrix}1&0\\1&1\end{pmatrix}\begin{pmatrix}1&0\\-1&1\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix},$$

$$\begin{pmatrix}1&-1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\-1&0\end{pmatrix}=\begin{pmatrix}2&1\\1&1\end{pmatrix}.$$

这就是说,取定 G/H 的两个元素

$$\left\{\begin{pmatrix}1&s\\1&s+1\end{pmatrix}\middle|s\in\mathbf{R}\right\},\quad \left\{\begin{pmatrix}1&s\\-1&1-s\end{pmatrix}\middle|s\in\mathbf{R}\right\},$$

当用

$$\begin{pmatrix}1&0\\1&1\end{pmatrix},\ \begin{pmatrix}1&0\\-1&1\end{pmatrix}$$

作代表时,$\bar{a}\#\bar{b}$ 是

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}H=H,$$

而用

$$\begin{pmatrix}1&-1\\1&0\end{pmatrix},\ \begin{pmatrix}1&1\\-1&0\end{pmatrix}$$

分别代表时,$\bar{a}\#\bar{b}$ 又该对应

$$\bar{c}=\begin{pmatrix}2&1\\1&1\end{pmatrix}H,$$

而矩阵

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

显然不在 H 中,故 $\bar{c} \neq H$, $\bar{a} \# \bar{b}$ 没有确定的意义,从而谈不上什么运算.

第二,商群 G/N 的运算 $\#$ 是专指定义 1 中指出的那个运算,它与 G 的运算自然地联系在一起,

$$aN \# bN = (a \circ b)N.$$

如果用其他运算将商集定义成群,那不是我们这里要求的 G 对 N 的商群.

例如,在整数加法群 I 中,所有能被 4 整除的数构成一个子群 N, N 是 I 的不变子群, N 所导出的等价关系就是模 4 关系, $m \sim n$ 当而且仅当 $m - n \in N$,而且商集

$$G/N = \{[0],[1],[2],[3]\}.$$

作为商群,其加法表是

⊞	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

它具有性质

$$[r] ⊞ [s] = [r + s].$$

当然,在商集 G/N 上还可以定义运算,

*	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[0]	[3]	[2]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[2]	[1]	[0]

且$(G/N, *)$也是群. 但这个群不能称为是 G 对 N 的商群.

下面举些商群的例子.

例 1 设 $G=\mathbf{S}_3, N=\langle(1\ 2\ 3)\rangle$. 由于

$$N=\{(1),(1\ 2\ 3),(1\ 3\ 2)\}\lhd G,$$

G/N 有两个元素,每个元素都是 G 的一个子集,精确说是 G 对 N 的陪集,即

$$G/N=\{\{(1),(1\ 2\ 3),(1\ 3\ 2)\},\{(1\ 2),\{1\ 3\},(3\ 2)\}\}.$$

乘法表是

*	$\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$	$\{(1\ 2),(1\ 3),(2\ 3)\}$
$\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$	$\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$	$\{(1\ 2),(1\ 3),(2\ 3)\}$
$\{(1\ 2),(1\ 3),(2\ 3)\}$	$\{(1\ 2),(1\ 3),(2\ 3)\}$	$\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$

例 2* 在 $\mathbf{I}_{12}$ 中取子群 $N_1=\{0^*,3^*,6^*,9^*\}$;在 $\mathbf{I}_4$ 中取子群 $N_2=\{0^*,2^*\}$. 那么 $N=N_1\times N_2$ 是 $\mathbf{I}_{12}\times\mathbf{I}_4$ 的一个不变子群.

$$N=\{(0^*,0^*),(3^*,0^*),(6^*,0^*),(9^*,0^*),(0^*,2^*),\\(3^*,2^*),(6^*,2^*),(9^*,2^*)\}.$$

G 是 48 元群,N 是 8 元群,G/N 应有 6 个元素,除 N 外还有

$$N_{1,0}=\{(1^*,0^*),(4^*,0),(7^*,0^*),(10^*,0^*),(1^*,2^*),\\(4^*,2^*),(7^*,2^*),(10^*,2^*)\},$$

$$N_{2,0}=\{(2^*,0^*),(5^*,0),(8^*,0^*),(11^*,0^*),(2^*,2^*),\\(5^*,2^*),(8^*,2^*),(11^*,2^*)\},$$

$$N_{1,1}=\{(1^*,1^*),(4^*,1^*),(7^*,1^*),(10^*,1^*),(1^*,3^*),\\(4^*,3^*),(7^*,3^*),(10^*,3^*)\},$$

$$N_{2,1}=\{(2^*,1^*),(5^*,1^*),(8^*,1^*),(11^*,1^*),(2^*,3^*),\\(5^*,3^*),(8^*,3^*),(11^*,3^*)\},$$

$$N_{0,1}=\{(0,1^*),(3^*,1^*),(6^*,1^*),(9^*,1^*),(0^*,3^*),\\(3^*,3^*),(6^*,3^*),(9^*,3^*)\}.$$

简单记,令 $N=N_{0,0}$,则

$$N_{0,0}=N, \qquad N_{0,1}=(0^*,1^*)+N,$$
$$N_{1,0}=(1^*,0^*)+N, \qquad N_{1,1}=(1^*,1^*)+N,$$
$$N_{2,0}=(2^*,0^*)+N, \qquad N_{2,1}=(2^*,1^*)+N.$$

其加法 # 表为

#	$N_{0,0}$	$N_{1,0}$	$N_{2,0}$	$N_{0,1}$	$N_{1,1}$	$N_{2,1}$
$N_{0,0}$	$N_{0,0}$	$N_{1,0}$	$N_{2,0}$	$N_{0,1}$	$N_{1,1}$	$N_{2,1}$
$N_{1,0}$	$N_{1,0}$	$N_{2,0}$	$N_{0,0}$	$N_{1,1}$	$N_{2,1}$	$N_{0,1}$
$N_{2,0}$	$N_{2,0}$	$N_{0,0}$	$N_{1,0}$	$N_{2,1}$	$N_{0,1}$	$N_{1,1}$
$N_{0,1}$	$N_{0,1}$	$N_{1,1}$	$N_{2,1}$	$N_{0,0}$	$N_{1,0}$	$N_{2,0}$
$N_{1,1}$	$N_{1,1}$	$N_{2,1}$	$N_{0,1}$	$N_{1,0}$	$N_{2,0}$	$N_{0,0}$
$N_{2,1}$	$N_{2,1}$	$N_{0,1}$	$N_{1,1}$	$N_{2,0}$	$N_{0,0}$	$N_{1,0}$

具体算法是

$$N_{m,n} \# N_{p,q}=[(m^*,n^*)+(p^*,q^*)]+N,$$

其中 $0\leqslant m,p<3$，$0\leqslant n,q<2$.

例 3 给定一个正方形如图 3－2. 用 $S=\{a,b,c,d\}$ 代表其顶点构成的集合. 我们看这个图形的运动. 注意，每次运动只要掌握了其顶点运动的情况，则整个图形的运动也就清楚了.

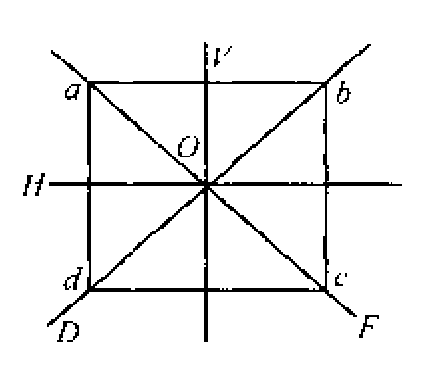


图 3－2

现在讨论运动后与运动前图形重合者. 这种运动实际上就是 S 上的一个置换. 由于 S 上的置换只有 $4!=24$ 个，这种运动最多有 24 个可能. 而实际上，有的置换不可能表示正方形的运动，比如要顶点 a,b 不动，而 c 变到 d，d 变到 c. 所以，能表示这种图形重合运动的置换只是 S 上置换中的一部分.

实际上，使四方形进行重合运动的有

$$\mu_1=\text{恒等置换},$$

μ_2 = 绕 O 顺时针转 90°，

μ_3 = 绕 O 顺时针转 180°，

μ_4 = 绕 O 顺时针转 270°，

μ_5 = 以 H 为轴翻转 180°，

μ_6 = 以 V 为轴翻转 180°，

μ_7 = 以 D 为轴翻转 180°，

μ_8 = 以 F 为轴翻转 180°.

任意二次使图形重合的运动合成后仍然是使该图形重合的运动，运动合成满足结合律；恒等置换是使图形重合的运动；每个使图形重合的运动都有逆运动使其恢复原样. 所以，

$$G=\{\mu_1,\mu_2,\mu_3,\mu_4,\mu_5,\mu_6,\mu_7,\mu_8\}$$

构成一个群. 其乘法表是

$\circ$	μ_1	μ_2	μ_3	μ_4	μ_5	μ_6	μ_7	μ_8
μ_1	μ_1	μ_2	μ_3	μ_4	μ_5	μ_6	μ_7	μ_8
μ_2	μ_2	μ_3	μ_4	μ_1	μ_7	μ_8	μ_6	μ_5
μ_3	μ_3	μ_4	μ_1	μ_2	μ_6	μ_5	μ_8	μ_7
μ_4	μ_4	μ_1	μ_2	μ_3	μ_8	μ_7	μ_5	μ_6
μ_5	μ_5	μ_8	μ_6	μ_7	μ_1	μ_3	μ_4	μ_2
μ_6	μ_6	μ_7	μ_5	μ_8	μ_3	μ_1	μ_2	μ_4
μ_7	μ_7	μ_5	μ_8	μ_6	μ_2	μ_4	μ_1	μ_3
μ_8	μ_8	μ_6	μ_7	μ_5	μ_4	μ_2	μ_3	μ_1

设 $N=\{\mu_1,\mu_3\}$，N 为 G 的子群，且对任意 $\mu\in G$，恒有

$$\mu\circ\mu_1\circ\mu^{-1}=\mu_1,\mu\circ\mu_3\circ\mu^{-1}=\mu_3,$$

所以，N 是 G 的不变子群，且

$$[\mu_2]=\mu_2\{\mu_1,\mu_3\}=\{\mu_2,\mu_4\},$$

$$[\mu_5]=\mu_5\{\mu_1,\mu_3\}=\{\mu_5,\mu_6\},$$

$$[\mu_7]=\mu_7\{\mu_1,\mu_3\}=\{\mu_7,\mu_8\}.$$

故 G 对 N 的商群 $G/N=\{[\mu_1],[\mu_2],[\mu_5],[\mu_7]\}$，即

$$G=\{\{\mu_1,\mu_3\},\{\mu_2,\mu_4\},\{\mu_5,\mu_6\},\{\mu_7,\mu_8\}\},$$

其乘法表是

#	$[\mu_1]$	$[\mu_2]$	$[\mu_5]$	$[\mu_7]$
$[\mu_1]$	$[\mu_1]$	$[\mu_2]$	$[\mu_5]$	$[\mu_7]$
$[\mu_2]$	$[\mu_2]$	$[\mu_1]$	$[\mu_7]$	$[\mu_5]$
$[\mu_5]$	$[\mu_5]$	$[\mu_7]$	$[\mu_1]$	$[\mu_2]$
$[\mu_7]$	$[\mu_7]$	$[\mu_5]$	$[\mu_2]$	$[\mu_1]$

例 4 设 G 是所有实的 2 阶可逆矩阵在矩阵乘法之下构成的群，N 是其中所有行列式为 1 的矩阵构成的子群. 那么，我们已经知道，N 是 G 的不变子群.

对任意矩阵 $A\in G$，设 $|A|=\alpha$. 由于 $\alpha\neq 0$，矩阵

$$B=\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}\in G,$$

而且 $|B^{-1}A|=|B|^{-1}|A|=\alpha^{-1}\alpha=1$，即 $B^{-1}A\in N$，$A\in BN$. 于是，集合

$$\left\{\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}\in G\,\middle|\,\alpha\in\mathbf{R}\right\}$$

是 G 对 N 的陪集表示的一个完全集，即

$$G/N=\left\{\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}N\,\middle|\,\alpha\in\mathbf{R}\right\}$$

其运算是

$$\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}N\#\begin{pmatrix}\beta & 0\\ 0 & 1\end{pmatrix}N=\begin{pmatrix}\alpha\beta & 0\\ 0 & 1\end{pmatrix}N.$$

命题 1 如果 G 是个群，N 是 G 的不变子群，那么映射 $f:G\to G/N$，

$$f(a)=aN,\quad 对任意\ a\in G,$$

是满同态映射，且 $\mathrm{Ker}(f)=N$.

证明 任取 $a,b\in G$，有

$$f(a\circ b)=(a\circ b)N=aN\# bN=f(a)\# f(b).$$

故 f 为 G 到 G/N 的同态映射.

进一步,G/N 中的任意元都是 G 对 N 的一个陪集,设为 aN, $a\in G$. 那么 $f(a)=aN$, f 是满的.

$(G/N,\#)$的恒等元是陪集 N. G 的元素 a, $a\in \mathrm{Ker}(f)$当而且仅当 $f(a)=N$,即

$$aN=N,$$

所以,$a\in \mathrm{Ker}(f)$当而且仅当 $a\in N$,从而有 $\mathrm{Ker}(f)=N$. ▌

这个同态映射通常称为 G 到 G/N 的**自然同态**.

例题 1 设 H 是群$(G,\circ)$的子群,在 G 对 H 左关系下的商集 G/H 中,规定,任意 aH, bH 对应 abH. 要使此规定合理,H 必须是 G 的不变子群.

证明 所谓"合理",就是指 aH, bH 对应 abH 与代表元选择无关,即对任意 $a_1,a_2\in G$ 和 $b_1,b_2\in G$,只要

$$a_1H=a_2H,\quad b_1H=b_2H.$$

则恒有$(a_1\circ b_1)H=(a_2\circ b_2)H$.

于是,对任意 $a\in G$ 及任意 $h\in H$,由于

$$aH=(ah)H,\quad a^{-1}H=a^{-1}H,$$

必有$(a\circ a^{-1})H=H=(a\circ h\circ a^{-1})H$,也就是 $a\circ h\circ a^{-1}\in H$, H 是 G 的不变子群. ▌

例题 2 设 N 是群 G 的不变子群. 那么,商群 G/N 为交换群的充分必要条件是对任意 $a,b\in G$,都有 $aba^{-1}b^{-1}\in N$.

证明 如果 G/N 是交换群,则对任意,$a,b\in G$, $aN,bN\in G/N$,应有

$$aN\# bN=bN\# aN,\quad (ab)N=(ba)N.$$

即$(ab)(ba)^{-1}\in N$,也就是 $aba^{-1}b^{-1}\in N$.

反过来,如果对任意 $a,b\in N$ 都有 $aba^{-1}b^{-1}\in N$,即 $ab(ba)^{-1}\in N$, ab 与 ba 在 N 的同一陪集中,也就是

$$abN=(a^{-1}b^{-1})^{-1}N=baN. \quad ▌$$

定理(同态基本定理) 设$(G,\circ)$和$(H,*)$都是群,f是G到H的满同态映射,$\mathrm{Ker}(f)=K$.那么有映射$\varphi:G/K\to H$,使得

$$\varphi(aK)=f(a),\quad 对每个\ aK\in G/K,$$

且φ是G/K到H的同构映射.从而$G/K\approx H$.

证明 先来定义G/N到H的映射φ.对任意$aK\in G/K$,令其对应H中的元素$f(a)$.这个规定表面上与aK的代表元选取有关.我们要证明定义是合理的,也就是要证明这个对应实际上与代表元选取无关.

如果$a_1K=a_2K$,则有$k\in K$使$a_1=a_2\circ k$,从而

$$f(a_1)=f(a_2\circ k)=f(a_2)*f(k)=f(a_2)*e_H=f(a_2),$$

就是说,$f(a)$是由aK唯一确定的,与代表元选取方法无关.

任取$aK,bK\in G/N$,有

$$\begin{aligned}
&\varphi(aK\# bK)\\
&\quad=\varphi((a\circ b)K) && (\#\text{的定义})\\
&\quad=f(a\circ b) && (\varphi\text{的定义})\\
&\quad=f(a)*f(b) && (f\text{是同态映射})\\
&\quad=\varphi(aK)*\varphi(bK). && (\varphi\text{的定义})
\end{aligned}$$

即φ是G/K到H的同态映射.

由于f是满射,对任意$h\in H$,必有$a\in G$使$f(a)=h$,从而$\varphi(aK)=h$.这说明φ是满同态.

要证明φ为单射,据上节命题8,我们只要证明$\mathrm{Ker}(\varphi)=\{e_{G/K}\}$. G/K的恒等元是K.设$aK\in G/K$, $\varphi(aK)=e_H$.即$aK\in\mathrm{Ker}\varphi$,那么

$$f(a)=\varphi(aK)=e_H.$$

由核的定义知$a\in\mathrm{Ker}(f)=K$,从而$aK=K$.也就是说$\mathrm{Ker}(\varphi)=\{e_{G/K}\}$. φ为单射.

所以,φ为G/K到H的双射同态,$G/K\approx H$. ∎

例题3* 条件如上面定理,再设$\gamma:G\to G/K$是G到G/K

的自然同态. 那么 $f=\varphi\circ\gamma$，也就是下面图形可换.

证明 要证明 G 到 H 的映射 f 和映射 $\varphi\circ\gamma$ 相等，只要证明它们作用在 G 的每个元素上效果都相同就行了.

图 3-3

对任意 $a\in G$，有

$$
\begin{aligned}
&(\varphi\circ\gamma)(a)\\
&\quad=\varphi[\gamma(a)] \quad \text{（映射合成的定义）}\\
&\quad=\varphi(aK) \quad \text{（}\gamma\text{ 是自然同态映射）}\\
&\quad=f(a), \quad \text{（}\varphi\text{ 的定义）}
\end{aligned}
$$

所以，$f=\varphi\circ\gamma$. ▌

例 5 看群 $(\mathbf{I},+)$ 和群 $(\mathbf{I}_n,+)$. §3 之例 5 表明，$f:\mathbf{I}\to\mathbf{I}_n$，

$$f(m)=r^*,\ m\in\mathbf{I},\quad m=nq+r,\ 0\leqslant r<n$$

是同态映射.

容易看出，f 是满同态.

计算 f 的核. 若 $f(m)=0^*$，则

$$m=qn+0,$$

即 m 是 n 的整数倍. 反之，若 m 是 n 的整数倍，亦必有 $f(m)=0^*$. 所以

$$K=\mathrm{Ker}(f)=\{\cdots,-n,0,n,\cdots\}=[0].$$

从而

$$G/K=\{[0],[1],\cdots,[n-1]\}=\mathbf{I}_{\sim n},$$

其中 $\mathbf{I}_{\sim n}$ 的运算规则是我们在第二章 §4 就已经讨论过了的. 于是，所得到的恰好就是现在定义的 G 对 K 的商群.

按同态基本定理，$\varphi:G/K\to\mathbf{I}_n$，

$$\varphi([m])=f(m),\quad m\in\mathbf{I}$$

是 $\mathbf{I}_{\sim n}$ 到 $\mathbf{I}_n$ 的同构映射.

由于 $\{0,1,\cdots,n-1\}$ 是 G 对 $[0]$ 的陪集表示的完全集，即对任意 $m\in\mathbf{I}$，设

$$m = nq + r, \quad 0 \leqslant r < n,$$

对$[m]=[r]$. 所以,φ 可以写成 $\varphi([r]) = r^*$, $0 \leqslant r < n$.

例 6 设 G,H 都是群,$G \otimes H$ 是它们的外直积,映射 $\pi: G \otimes H \to G$,

$$\pi((g,h)) = g, \quad \text{对每个}(g,h) \in G \times H$$

是个同态映射(见 §3 例 4).

这是满同态,且

$$\mathrm{Ker}(f) = H' = \{(g,h) \in G \otimes H \mid g = e_G\}.$$

据同态基本定理$(G \otimes H)/H' \approx G$.

例题 4 决定例 3 中所给的使图 3-2 中正方形重合的运动构成的群 G 的所有同态像(同构的群看成是相同的同态像).

解 由同态基本定理知,这等价于决定 G 的商群,又等价于决定 G 的所有不变子群.

G 的阶数是 8, G 的非平凡子群的阶数只能是 2 和 4.

对于平凡子群 G 和 $\{e\}$,显然

$$G/G \approx \{e\}, \quad G/\{e\} \approx G.$$

现在只要决定 G 的非平凡的正规子群.

如果 H 是 G 的 4 阶子群,那么

$$8 = |G| = 2|H|,$$

G/H 是 2 阶群,而所有 2 阶群都是同构的,于是 $G/H \approx \mathbf{I}_2$, $\mathbf{I}_2$ 是 G 的一个同态像.

G 有 4 阶子群,$\langle \mu_2 \rangle$就是一个,剩下的问题是决定 G 的 2 阶子群.

2 阶子群必为循环群,由阶为 2 的元素生成. 而 G 中阶数为 2 的元素有

$$\mu_3, \mu_5, \mu_6, \mu_7, \mu_8.$$

看商群 $G/\langle \mu_3 \rangle$. 它有 4 个元素,即$\{\mu_1, \mu_3\}$和

$$\mu_2\{\mu_1, \mu_3\}, \mu_5\{\mu_1, \mu_3\}, \mu_7\{\mu_1, \mu_3\}.$$

例 3 所给的 $G/\langle\mu_3\rangle$ 的乘法表中表明，它的每个非恒等元的周期都是 2. 3 个非恒等元中的任意两个的积恰好等于另外一个元素. 故由 §1 的例题知

$$G/\langle\mu_3\rangle \approx \mathbf{I}_2 \otimes \mathbf{I}_2.$$

而 $\langle\mu_5\rangle$, $\langle\mu_6\rangle$, $\langle\mu_7\rangle$ 和 $\langle\mu_8\rangle$ 都不是 G 的不变子群. 所以，G 的同态像是 G, $\mathbf{I}_2$, $\mathbf{I}_2 \otimes \mathbf{I}_2$, $\mathbf{I}_1$. ▮

例题 5 设 G 是个群. 那么 G 的中心

$$C = \{g \in G \mid ga = ag, \text{对每个 } a \in G\}$$

是 G 的不变子群，而且 G/C 同构于 G 的所有内自构作成的群 H.

证明 先证明 C 是 G 的子群. 对任意 $a \in G$，由 $e_G a = a e_G = a$，知 $e_G \in C$. 如果 $g, h \in C$，那么对任意 $a \in G$，有

$$a(gh) = (ag)h = (ga)h = g(ha) = (gh)a,$$

因而 $gh \in C$. 如果 $g \in C$，即对任意 $a \in G$，$ag = ga$. 将此式两端两侧同乘 g^{-1}，则得

$$g^{-1}agg^{-1} = g^{-1}a = ag^{-1} = g^{-1}gag^{-1}.$$

这说明 $g^{-1} \in C$. 所以，C 是 G 的子群.

进一步，对任意 $a \in G$ 及 $g \in C$，都有

$$aga^{-1} = g(aa^{-1}) = g \in C,$$

从而 C 还是 G 的不变子群.

在 §2 的命题 5 中，我们用 γ_a 代表 G 中元素 a 所导出的 G 到 G 的内自同构映射.

$$\gamma_a(x) = axa^{-1}, \quad \text{对每个 } x \in G.$$

由于 G 到 G 的恒等自同构等于 γ_e，必为内自同构；任意两个内自同构 γ_a 和 γ_b 的合成，有

$$(\gamma_a \circ \gamma_b)(x) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = \gamma_{ab}(x),$$

即 $\gamma_a \circ \gamma_b$ 也是内自同构；对任意内自同构 γ_a，都有 $\gamma_a \circ \gamma_{a^{-1}} = \gamma_e$. 所以，所有内自同构的集合 H 在映射合成之下作成一个群，

$$H = \{\gamma_a \mid a \in G\}.$$

这里要注意，H 中的元素是由 G 中元素导出来的，并不是用 G 来标号；也就是说，G 中元素 $a \neq b$，但可能使 $\gamma_a = \gamma_b$.

现在来建立一个 G 到 H 的映射 f，

$$f(a) = \gamma_a, \quad \text{对每个 } a \in G.$$

对任意 $a, b \in G$，有

$$\begin{aligned} & f(ab) \\ & = \gamma_{ab} && (f \text{ 的定义}) \\ & = \gamma_a \circ \lambda_b && (\lambda_{ab}(x) = (\lambda_a \circ \lambda_b)(x), \text{每个 } x \in G) \\ & = f(a) \circ f(b). && (f \text{ 的定义}) \end{aligned}$$

所以，f 是同态映射.

因为 H 中的任意元素 γ_a 都是 G 中某元导出来的，$f(a) = \gamma_a$，故 f 是满的.

再来计算 f 的核. H 的恒等元是 G 到 G 的恒等映射 i_G. 如果 $a \in G$，$a \in \mathrm{Ker}(f)$，即 $f(a) = i_G$，那么对任意 $x \in G$，必有

$$f(a)(x) = \gamma_a(x) = axa^{-1} = i_G(x) = x.$$

从而有

$$ax = xa, \quad \text{对每个 } x \in G,$$

也就是 $a \in C$. 反之，$a \in C$，则对每个 $x \in G$ 有

$$ax = xa, \quad axa^{-1} = a,$$

从而 $\gamma_a = i_G$，$\gamma_a \in \mathrm{Ker}(f)$.

所以，$\mathrm{Ker}(f) = C$.

由同态基本定理，得 $G/C \approx H$. ▌

下面的例题是深入学习群论时的一个重要的基础性定理（称为第二同构定理）. 但在自学阶段，只要求读者领会其证明技巧，而不要求每人都能自如地运用它.

例题 6* 设 H 和 K 都是群 G 的不变子群，且 $K \lhd H$. 证明：H/K 是 G/K 的不变子群，且 $(G/K)/(H/K) \approx G/H$.

证明 我们用$\circ$表示 G 的运算，$\#$ 表示商群 G/K 的运算，γ 表示G 到G/K 的自然映射，$\gamma(a)=aK$，对每个 $a\in G$.

由于 $H\lhd G$，γ 是满的，由 §3 命题 6 可知 $\gamma(H)\lhd G/K$. 现拟证明

$$H/K=\gamma(H).$$

事实上，任意 $h\in H$，则

$$\gamma(h)=hK\in H/K.$$

而对每个 $hK\in G/K$，$h\in H$，必有

$$hK=\gamma(h)\in\gamma(H).$$

所以，$\gamma(H)=H/K$，H/K 是G/K 的一个不变子群.

于是又有 G/K 到其商群$(G/K)/(H/K)$的自然映射 ρ，

$$\rho(aK)=aK\#(H/K),\quad 对每个\ aK\in G/K.$$

由于 $\gamma:G\to G/K$ 是同态映射，$\rho:G/K\to(G/K)/(H/K)$也是同态映射. 所以 $\rho\circ\gamma$ 是群 G 到群$(G/K)/(H/K)$的同态映射(§3 命题 4).

而且，因为 γ 和 ρ 都是满射，所以 $\rho\circ\gamma$ 也是满射.

再来计算映射 $\rho\circ\gamma$ 的核. 据 §3 定理 1，

$$\mathrm{Ker}(\rho\circ\gamma)=\gamma^{-1}\mathrm{Ker}(\rho).$$

而 ρ 是自然同态，故 $\mathrm{Ker}(\rho)=H/K$. 从而

$$\mathrm{Ker}(\rho\circ\gamma)=\gamma^{-1}(H/K).$$

我们要证明 $\gamma^{-1}(H/K)=H$. 由于 γ 是自然同态，$\gamma(H)\subseteq H/K$，故

$$\gamma^{-1}(H/K)\supseteq H.$$

反之，若 $a\in G$，$a\in\gamma^{-1}(H/K)$，即

$$\gamma(a)=aK\in H/K,$$

即必有 $h\in H$，使得 $aK=hK$，$ah^{-1}\in K$. 进而

$$a=(ah^{-1})h\in H,$$

因为 H 是G 的子群. 这说明 $\gamma^{-1}(H/K)\subseteq H$.

总之，$\gamma^{-1}(H/K)=H$，而且 $\mathrm{Ker}(\rho\circ\gamma)=H$. 据同态基本定理，得到 $G/H\approx(G/K)/(H/K)$. ▌

看一个实例，设 $G=(I,+)$，$H=\langle 4\rangle$，$K=\langle 8\rangle$. 于是，G/K有 8 个元素，即 G 对 K 的 8 个陪集

$$\langle 8\rangle,1+\langle 8\rangle,2+\langle 8\rangle,3+\langle 8\rangle,4+\langle 8\rangle,$$
$$5+\langle 8\rangle,6+\langle 8\rangle,7+\langle 8\rangle,$$

按我们常用的符号记，乃是

$$G/K=\{[0],[1],[2],[3],[4],[5],[6],[7]\}.$$

而 H/K 是G/K 的不变子群，它的元素是

$$\langle 8\rangle,4+\langle 8\rangle,$$

也就是 $H/K=\{[0],[4]\}$.

进而$(G/K)/(H/K)$的元素是 G/K 对 H/K 的陪集，它的元素是

$$\{[0],[4]\},\ [1]+\{[0],[4]\},\ [2]+\{[0],[4]\},$$
$$[3]+\{[0],[4]\}.$$

将其分别记为$[[0]],[[1]],[[2]],[[3]]$，其运算表应为

+	[[0]]	[[1]]	[[2]]	[[3]]
[[0]]	[[0]]	[[1]]	[[2]]	[[3]]
[[1]]	[[1]]	[[2]]	[[3]]	[[0]]
[[2]]	[[2]]	[[3]]	[[0]]	[[1]]
[[3]]	[[3]]	[[0]]	[[1]]	[[2]]

同时，G/H 有 4 个元素，即

$$\langle 4\rangle,1+\langle 4\rangle,2+\langle 4\rangle,3+\langle 4\rangle,$$

我们用$[0]',[1]',[2]',[3]'$分别表示之.

要注意 G/K 中的$[1]$和 G/H 中的$[1]'$是有区别的，

$$[1]=\{\cdots,1,9,17,\cdots\},\quad [1]'=\{\cdots,1,5,9,\cdots\}.$$

群 G/H 的运算表为

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

在一个群 G 中,有时对某些特殊元素无法驾驭,把它们集中到一个不变子群 N 中,商群 G/N 就不含这种特殊元素了,研究起来就方便些了.

例题 7 设 G 是个交换群.证明:G 的所有阶数有限的元素的集合 N 是 G 的一个不变子群,且商群 G/N 的非恒等元的阶数都是无限的.

证明 $a\in G$, a 阶数有限的充分必要条件是有正整数 k 使得

$$a^k = e.$$

任取 $a, b\in N$,设有正整数 k, l 使

$$a^k = e,\quad b^l = e.$$

那么 $(ab)^{kl} = a^{kl}b^{kl} = (a^k)^l(b^l)^k = e$,从而知 $ab\in N$.

又,a 和 a^{-1} 的阶数恒相同,当 $a\in N$ 时必有 $a^{-1}\in N$.

所以 N 是 G 的子群.又由于 G 是交换群,N 还是 G 的不变子群.

任取商群 G/N 的一个元素 gN,若 gN 之阶数有限,则必有正整数 k 使

$$N=(gN)^k = g^kN,$$

从而知 $g^k\in N$.但 N 中元素都是有限阶的,又必有正整数 l 使 $(g^k)^l = e$,也就是 $g^{kl} = e$.这说明,g 本身就是 N 中的元素,$gN=N$.也就是说,gN 必然是商群 G/N 的恒等元才行,而非恒等元之阶数必无限. ▌

例题 8* 用 $\mathbf{C}^{\#}$ 代表所有非零复数构成的乘法群,用 $\mathbf{R}^{+}$ 代表所有正实数构成的乘法群.讨论 $\mathbf{C}^{\#}$ 和 $\mathbf{R}^{\#}$ 的关系.

证明 任意非零复数 α 可唯一的表成

$$\alpha = r(\cos\theta + \mathrm{i}\sin\theta),\quad 0 \leqslant \theta < 2\pi$$

形式,其中 $r = |\alpha|$ 称为是 α 的模.规定

$$\sigma: \alpha \to r = |\alpha|,\quad \alpha \in \mathbf{C}^{\#}.$$

则 σ 是 $\mathbf{C}^{\#}$ 到 $\mathbf{R}^{+}$ 的一个映射.

对任意 $\alpha, \beta \in \mathbf{C}^{\#}$,由于 $|\alpha\beta| = |\alpha||\beta|$,故

$$\sigma(\alpha\beta) = |\alpha\beta| = |\alpha||\beta| = \sigma(\alpha)\sigma(\beta),$$

这说明 σ 是同态映射.

每个非零实数 r 都是它本身的模 $|r| = r$.所以,σ 还是满的.

现在看 $\mathrm{Ker}(\sigma)$.若 $\sigma(\alpha) = |\alpha| = 1$,则 $\alpha = \cos\theta + \mathrm{i}\sin\theta$.令

$$N = \mathrm{Ker}(\sigma) = \{r \in \mathbf{C}^{\#} \mid r = \cos\theta + \mathrm{i}\sin\theta\},$$

由群同态基本定理得 $\mathbf{C}^{\#}/N \cong \mathbf{R}^{+}$.

同样办法可得

$$\mathbf{C}^{\#}/\mathbf{R}^{+} \cong N. \qquad \blacksquare$$

这样,关于复平面非零复数的乘法的讨论可以利落地分成两部分,一是正实数乘法,一是单位圆上之二复数相乘.把大问题化成了比较小的问题.把一个平面(除零点外)问题化成了一个射线和一个单位圆来讨论.

例题 9 证明:实数加法群 $\mathbf{R}$ 到 2 阶非奇异实矩阵的乘法群 $M_{2\times 2}(\mathbf{R})$上的映射

$$\sigma: x \to \begin{pmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{pmatrix},\quad x \in \mathbf{R}$$

是个同态映射并求 $\mathrm{Ker}(\sigma)$.

证明 对任意 $x, y \in \mathbf{R}$,因为

$$\begin{aligned}\sigma(x+y) &= \begin{pmatrix} \cos(x+y) & \sin(x+y) \\ -\sin(x+y) & \cos(x+y) \end{pmatrix} \\ &= \begin{pmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{pmatrix}\begin{pmatrix} \cos y & \sin y \\ -\sin y & \cos y \end{pmatrix} \\ &= \sigma(x)\cdot\sigma(y),\end{aligned}$$

故 σ 是 $\mathbf{R}$ 到 $M_{2\times 2}(\mathbf{R})$的一个同态映射.

对任意 $x\in\mathbf{R}$, $x\in\operatorname{Ker}(\sigma)$的充分必要条件是

$$\sigma(x)=\begin{pmatrix}\cos x & \sin x\\ -\sin x & \cos x\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},$$

即 $\cos x=1$, $\sin x=0$,即 $x=2k\pi$.所以 $\operatorname{Ker}(\sigma)=\{2k\pi\mid k\in\mathbf{I}\}$. ▌

习 题 四

1. 给出对称群 $\mathbf{S}_3$ 的所有非平凡的不变子群及相应的商群.

2. 给出克莱因四元数群(§2 之例题 8)的所有非平凡不变子群及其相应的商群.

3. 证明:$G=\{2^n5^m\mid m,n\in\mathbf{I}\}$ 在数的乘法之下构成群,而 $N=\{2^n\mid n\in\mathbf{I}\}$是 G 的不变子群,并且给出商群 G/N 的结构.

4*. 给出加群 $\mathbf{I}\times\mathbf{I}$ 对其子群 $N=\{(m,-m)\mid m\in\mathbf{I}\}$的商群 G/N 的结构(参见习题三之题 5).

5*. 用 Z 代表群 G 的中心.若商群 G/Z 是循环群,则 G 本身必然是交换群.

§5* 群的内直积和外直积

在第二章§6 里,我们可以把任意两个本来没有内在关联的群(G,Δ)和$(H,\circ)$硬性地"拼凑"到一起作成一个群$(G\times H,\otimes)$.这个群的结构尤如一个松散的联邦,元素运算按 G 的运算和 H 的运算分别进行.即,对任意$(a,x),(b,y)\in G\times H$,有

$$(a,x)\otimes(b,y)=(a\Delta b,x\circ y).$$

对于 G 和 H 的外直积$G\otimes H$,已知这样一些性质:

(1) 集合

$$G'=\{(g,h)\in G\times H\mid h=e_H\}$$

是 $G\otimes H$ 的一个不变子群,且 $G'\approx G$.

(2) 集体

$$H'=\{(g,h)\in G\times H\mid g=e_G\}$$

也是 $G\otimes H$ 的一个不变子群,且 $H'\approx H$.

(3) $G\otimes H=G'H'=H'G'$.

其中(3)意味着 $G\otimes H$ 的每个元素都是 G' 中一个元和 H' 中一个元的乘积. 这是自然的,因为对任意 $(g,h)\in G\otimes H$,有

$$(g,h)=(g,e_H)\otimes(e_G,h).$$

实际上,$G\otimes H$ 的元素表成 G' 元与 H' 元之积的表示方法是唯一的. 因为若某元有两种表法如下

$$(g_1,e_H)\otimes(e_G,h_1)=(g_2,e_H)\otimes(e_G,h_2),$$

则必有 $(g_1,h_1)=(g_2,h_2)$. 笛卡尔积中元素相等的充分必要条件是所有分量都相等,故得

$$g_1=g_2,\quad h_1=h_2,$$

$$(g_1,e_H)=(g_2,e_H),\ (e_G,h_1)=(e_G,h_2).$$

所以,还有

(4) $G\otimes H$ 的每个元素恒可唯一地表成 G' 与 H' 的元素之积.

G 和 H 可能本无内在关联. 但 G', H' 却是同一个群的子群. 对于这种情形,有

定义 1 设 G 是个群, A 和 B 是 G 的子群,且满足条件

(1) A, B 都是 G 的不变子群,

(2) 对任意 $g\in G$,都有唯一确定的 $a\in A$ 和 $b\in B$ 使得 $g=ab$,则说群 G 是其子群 A 和子群 B 的**内直积**.

命题 1 对任意群 G 和 H,其外直积 $G\otimes H$ 是其子群 G' 和子群 H' 的内直积,其中

$$G'=\{(g,h)\in G\times H \mid h=e_H\},$$

$$H'=\{(g,h)\in G\times H \mid g=e_G\}.$$ ▌

例 1 四元群 $G=\{e,a,b,c\}$ 的乘法表是

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

它有3个2阶不变子群 $K=\{e,a\}$, $H=\{e,b\}$和 $L=\{e,c\}$,而且 G 是其中任意两个不同的不变子群的内直积.

因为有对称性,我们只看 K 和 H 就行了.

事实上,

$$a=ae,\quad b=eb,\quad c=ab,\quad e=ee,$$

即 $G=KH$,而且表法唯一.也就是说,K 和 H 满足定义要求的条件,G 是 K 和 H 的内直积.

例2 设循环群 $G=\langle g\rangle$ 的阶数为 n,而且 $n=pq$, p 和 q 互素,那么 G 是其子群 $\langle g^p\rangle$ 和 $\langle g^q\rangle$ 的内直积.

这是因为,由 p,q 互素知必有整数 i,j 使

$$ip+jq=1,$$

从而对任意 $g^m\in G$,都有

$$g^m=g^{pim}g^{qjm},$$

其中 $g^{pim}\in\langle g^p\rangle$, $g^{qjm}\in\langle g^q\rangle$.这说明 G 的元素恒为一个 $\langle g^p\rangle$ 元素与一个 $\langle g^q\rangle$ 中元素的乘积.

设有 G 的元素写成 $\langle g^p\rangle$ 与 $\langle g^q\rangle$ 元素积时有2个表示方法, $g^{ps}g^{qt}$ 和 $g^{pk}g^{ql}$,即

$$g^{ps+qt}=g^{pk+ql}. \tag{1}$$

那么,由于 g 的阶数为 n,必有 $n\mid(p(s-k)+q(t-l))$.

由于 $n=pq$, $p\mid(p(s-k))$,所以

$$p\mid(q(t-l)).$$

但是,p 和 q 互素,这就必然有 $p\mid(t-l)$.于是 $pq=n$ 能整除 $q(t-l)$,而 g 的阶为 n,故

$$g^{q(t-l)}=e,\quad g^{qt}=g^{ql}.$$

同理,$g^{ps}=g^{pk}$.

这说明(1)中元素的2个表法是一样的.

每个循环群都是交换群,交换群的子群都是不变子群,$\langle g^p\rangle$ 和 $\langle g^q\rangle$ 都是 $\langle g\rangle$ 的不变子群.

总之,G 是 $\langle g^p\rangle$ 和 $\langle g^q\rangle$ 的内直积.

对于交换群,有时将外直积和内直积分别称为外直和和内直和,并用$\oplus$代替$\otimes$.

例 3 整数加法群$(\mathbf{I},+)$不是它的两个非平凡子群的内直和.

设$\mathbf{I}$是子群K和子群H的内直和.我们知道,$\mathbf{I}$的每个子群都是由一个元素生成的.设

$$K=\langle m\rangle,\quad H=\langle n\rangle$$

且m,n都不等于0.

G之每个元可由$\langle m\rangle$和$\langle n\rangle$元素表示出来,设有整数s和t使得

$$1=sm+tn,\quad sm\in\langle m\rangle,\ tn\in\langle n\rangle.$$

那么,必然还有

$$1=(s+n)m+(t-m)n,\ (s+n)m\in\langle m\rangle,\ (t-m)n\in\langle n\rangle.$$

由于m,n均不为0,故

$$s+n\neq s,\ t-m\neq t,$$

这说明$\mathbf{I}$的元素1有两种不同的表法.

下面给出一些判别群为其子群之内直积的方法.

命题 2 设G是个群,A,B是它的不变子群.那么,G为A,B之内直积的充分必要条件是$G=AB$,且G之恒等元e写成A元和B元之积时表法唯一.

证明 如果G是A和B的内直积,据定义1,它满足条件1°和2°,它的任意元g表成

$$g=ab,\quad a\in A,\ b\in B$$

时,表法唯一,特别地,e表成A元与B元之积时表法唯一.

反过来,若$G=AB$,则G之每元g均有

$$g=ab,\quad a\in A,\ b\in B, \tag{2}$$

我们要证明,只要e的表法唯一,则任意元g的表法必唯一.

设还有$c\in A,\ d\in B$使$g=cd$,于是

$$ab=cd,$$

$$e = a^{-1}(cd)b^{-1} = (a^{-1}c)(db^{-1}). \tag{3}$$

由于 A,B 均为 G 之子群,故

$$a^{-1}c \in A, \quad db^{-1} \in B.$$

这就导致 e 有两种表示方法,(3)和

$$e = ee, \quad e \in A,\ e \in B.$$

由 e 表法唯一的假定,推出

$$a^{-1}c = e,\ db^{-1} = e,$$

也就是 $a = c,\ d = b$.所以,上面给出的 g 的两种表法实际上是相同的.

G 为 A,B 的内直积. ∎

命题3 设 G 是个群,A,B 是它的不变子群.那么 G 是 A 与 B 的内直积的充分必要条件是 $G = AB$,且 $A \cap B = \{e\}$.

证明 与命题1比较,我们只要证明,在 A 和 B 均为不变子群,且 $G = AB$ 的前提下,

$$A \cap B = \{e\}$$

与 e 的表法唯一是等价的.

事实上,若有 $g \in A \cap B,\ g \neq e$,那么

$$e = ee = gg^{-1}, \quad g \in A,\ g^{-1} \in B$$

就是两种不同的表法.

反之,若 e 还有除 $e = ee$ 外的另一种不同表法,设

$$e = gh, \quad g \in A,\ h \in B,$$

其中 g 和 h 至少有一个不等于 e(实际上,有一个不等于 e,则另一个元素亦必不等于 e),不妨设 $g \neq e$,于是有

$$g^{-1} = h,$$

由 $h \in B$ 知 $g^{-1} \in B$.但 B 为子群,故 $g \in B,\ g \in A \cap B$,而且 $g \neq e$,所以,$A \cap B \neq \{e\}$. ∎

定理1 设 G 是个群,A 和 B 是 G 的子群.那么,G 为 A 与 B 的内直积的充要条件是

1° 对任意 $a \in A,\ b \in B$ 都有 $ab = ba$;

2^*　对每个 $g\in G$，都有 $a\in A$，$b\in B$ 使 $g=ab$，而且表法唯一.

证明　对照内直积的定义.我们只要证明，当 A,B 是群 G 的子群且满足条件 2^* 时，条件 1^* 与 A,B 是 G 的不变子群等价.

如果 A 和 B 满足 1^*，那么，对任意 $g\in G$，任意 $x\in A$，设 $g=ab$，$a\in A$，$b\in B$（条件 2^*），就有

$$\begin{aligned}
&gxg^{-1}\\
&\quad = abxb^{-1}a^{-1} && (g=ab)\\
&\quad = a(bb^{-1})xa^{-1} && (A\text{ 中元与 }B\text{ 中元可换})\\
&\quad = axa^{-1} && (bb^{-1}=e)\\
&\quad \in A. && (a,x\text{ 均在 }A\text{ 中})
\end{aligned}$$

从而证明了 A 是 G 的不变子群.

同理，B 也是 G 的不变子群.

由定义 1 即知 G 是 A 和 B 的内直积.

反过来，如果 G 是其子群 A 和 B 的内直积，那么，对任意 $a\in A$，$b\in B$，都有

$$(aba^{-1})b^{-1}=a(ba^{-1}b^{-1}). \tag{4}$$

由于 B 是 G 的不变子群，故 $aba^{-1}\in B$，从而

$$(aba^{-1})b^{-1}\in B.$$

由于 A 是 G 的不变子群，故 $ba^{-1}b^{-1}\in A$，进而

$$a(ba^{-1}b^{-1})\in A.$$

这说明 $aba^{-1}b^{-1}\in A\cap B$. 据命题 2，$A\cap B=\{e\}$. 所以，

$$aba^{-1}b^{-1}=e,\quad ab=ba.$$

也就是说 G 为 A,B 之内直积蕴涵着满足条件 1^* 和 2^*. ▌

例题 1　设群 G 是其子群 A,B 的内直积，且

$$C=\{x\in G\mid xg=gx\text{ 对所有 }g\in G\},$$
$$D=\{y\in A\mid ya=ay\text{ 对所有 }a\in A\},$$
$$E=\{z\in B\mid zb=bz\text{ 对所有 }b\in B\}.$$

那么，C 是 D 和 E 的内直积.

证明 D 是A 的子群,从而也是 G 的子群.同样,E 是G 的子群.

若 $y\in D$,则对任意 $g\in G$, $g=ab$ (G 是A 和B 的内直积), $a\in A$, $b\in B$有

$$
\begin{aligned}
& y(ab) \\
&=(ya)b && (\text{结合律}) \\
&=(ay)b && (y\in D,\ a\in A) \\
&=(ab)y. && (\text{定理 } 1,\ ab=ba)
\end{aligned}
$$

从而 $y\in C$.所以,D 是C 的子群.

同理,E 是C 的子群.

对任意 $x\in C$,由于 $C\subseteq G$, G 是A,B 的内直积,必有 $u\in A$,$v\in B$ 使

$$
x=uv. \tag{5}
$$

对任意 $a\in A$,有

$$
\begin{aligned}
ax &= xa, && \\
auv &= uva, && (G\text{ 是}A,B\text{ 内直积}(5)) \\
auv &= uav, && (\text{定理 }1,A\text{ 元与}B\text{ 元可换}) \\
au &= ua. && (\text{群中消去律})
\end{aligned}
$$

这说明 $u\in D$.

同理 $v\in E$.

所以,C 中元恒可写成 D 元与 E 元之积.其表法自然是唯一的,因为 C 元写成 A 元与 B 元之积时表法唯一,而 $D\subseteq A$, $E\subseteq B$. ▌

现在,我们来研究内直积概念和外直积概念的关系.

本节开初叙述的事实,乃是说,任意两个群 G 和H 恒可做一外直积$G\otimes H$,$G\otimes H$ 恰为其子群G'和H'的内直积,且

$$
G'\approx G, \quad H'\approx H.
$$

这说是命题 1.

同时,反过来,还有

命题 4 若群 G 是其子群A,B 的内直积,则 $G\approx A\otimes B$.

证明 建立 A,B 的外直积 $A\otimes B$ 到 G 的映射 φ，对任意 $(a,b)\in A\times B$，令 $\varphi((a,b))=ab$.

φ 是单射. 因为若有 $a,a'\in A$, $b,b'\in B$ 使

$$\varphi((a',b'))=\varphi((a,b))$$

即 $ab=a'b'$，那么，由于 G 是 A,B 的内直积，据表法唯一性，必有 $a=a'$, $b=b'$，即 $(a',b')=(a,b)$.

φ 是满射. 因为对任意 $g\in G$，必有 $a\in A$ 和 $b\in B$ 使得 $g=ab$ (G 是 A,B 内直积)，即 $g=\varphi((a,b))$, $(a,b)\in A\times B$.

φ 还是个同态映射. 对任意 $(a,b),(a',b')\in A\times B$ 都有

$$\begin{aligned}
&\varphi((a,b)\otimes(a',b'))\\
&=\varphi((aa',bb')) &&(\text{外直积元素乘法})\\
&=(aa')(bb') &&(\varphi\ \text{的定义})\\
&=(ab)(a'b') &&(A\ \text{元与}\ B\ \text{元可换})\\
&=\varphi((a,b))\varphi((a',b')). &&(\varphi\ \text{的定义})
\end{aligned}$$

所以，$A\otimes B\approx G$. ▌

由于同构的群的代数结构完全一样，有些书上对内直积和外直积不加区别，一律简单记成 $A\times B$ 的样子，把同构符号索性写成相等. 这常常引起初学者的迷惑. 大家遇到这类习题时要首先区别内外，再用命题 1 和命题 4 作精确同构性解释.

§2 末例题中，任意群 G 中形如

$$a_1b_1a_1^{-1}b_1^{-1}\cdots a_nb_na_n^{-1}b_n^{-1},\quad n=1,2,\cdots$$

构成的不变子群 X (称为 G 的**换位子群**). 我们介绍如下的习题，试分析之.

例题 2 直积 $A\times B$ 的换位子群等于 A,B 的换位子群的直积.

证法 1 设群 G 是其子群 A,B 的内直积. 用 X,Y,Z 分别代表 G,A,B 的换位子群. 因为 A,B 是 G 的子群，Z 和 Y 的元素也是 X 中的元素，所以 Y 和 Z 是 X 的子群.

由于 A 和 B 的元素可交换，当然 Y 和 Z 的元素亦可换.

对任意 $x\in X$,设

$$x=g_1h_1g_1^{-1}h_1^{-1}\cdots g_nh_ng_n^{-1}h_n^{-1},$$
$$g_1,\cdots,g_n,h_1,\cdots,h_n\in G;\ n\in \mathbf{I}.$$

由于 G 是 A 和 B 的内直积,故有

$$a_1,\cdots,a_n,c_1,\cdots,c_n\in A;\quad b_1,\cdots b_n,d_1,\cdots,d_n\in B,$$

使得

$$g_1=a_1b_1,\ \cdots,\ g_n=a_nb_n,\ h_1=c_1d_1,\ \cdots,\ h_n=c_nd_n.$$

于是,由于 A 元与 B 元可换,可得

$$x=(a_1c_1a_1^{-1}c_1^{-1}\cdots a_nc_na_n^{-1}c_n^{-1})(b_1d_1b_1^{-1}d_1^{-1}\cdots b_nd_nb_n^{-1}d_n^{-1}),$$

即 x 为 Y 中元与 Z 中元的乘积.

剩下来要证明的是 X 元表成 Y 元与 Z 元的乘积时,表法唯一.

因为 G 是 A 和 B 的内直积,X 中元作为 G 中元表成 A 元和 B 元之积时,表法唯一,而 Y 元在 A 中,Z 元在 B 中,故 X 元表成 Y 元与 Z 元之积时,表法唯一.

这里要注意,换位子群的元素表成

$$g_1h_1g_1^{-1}h_1^{-1}\cdots g_mh_mg_m^{-1}h_m^{-1}$$

形式时表法可能并不唯一.在我们证明 X 是 Y 和 Z 的内直积时,只要求,若

$$x=y_1z_1=y_2z_2,\quad y_1,y_2\in Y,\ z_1,z_2\in Z$$

必有 $y_1=y_2$ 和 $z_1=z_2$.至于诸 y 和 z 在 Y 和 Z 的内部如何表达出来,与本题要求无关.

证法 2 设 A,B 是群,G 是 A,B 的外直积 $G=A\otimes B$.用 X,Y,Z 分别代表 G,A,B 的换位子群.

对任意 $g\in X$;设

$$g=(a_1,b_1)(c_1,d_1)(a_1,b_1)^{-1}(c_1,d_1)^{-1}\cdots(a_n,b_n)\cdot(c_n,d_n)(a_n,b_n)^{-1}(c_nd_n)^{-1}$$

按外直积的乘法规则,有

$$g=(a_1c_1a_1^{-1}c_1^{-1}\cdots a_nc_na_n^{-1}c_n^{-1},b_1d_1b_1^{-1}d_1^{-1}\cdots b_nd_nb_n^{-1}d_n^{-1}),$$

从而 $g\in Y\otimes Z$.

反之,若 $g\in Y\otimes Z$,设有 $a_i,c_i\in Y$, $b_j,d_j\in Z$ 使

$$g=(a_1c_1a_1^{-1}c_1^{-1}\cdots a_nc_na_n^{-1}c_n^{-1},b_1d_1b_1^{-1}d_1^{-1}\cdots b_md_mb_m^{-1}d_m^{-1}).$$

若 $m\neq n$,不妨设 $m<n$,再令

$$d_{m+1}=b_{m+1}=e,\quad \cdots,\quad d_n=b_n=e,$$

把两个分量配成整齐的样子,即

$$g=(a_1c_1a_1^{-1}c_1^{-1}\cdots a_nc_na_n^{-1}c_n^{-1},b_1d_1b_1^{-1}d_1^{-1}\cdots b_md_mb_m^{-1}d_m^{-1}\cdots b_nd_nb_n^{-1}d_n^{-1}).$$

按外直积运算规则,有

$$g=(a_1,b_1)(c_1,d_1)(a_1,b_1)^{-1}(c_1,d_1)^{-1}\cdots(a_n,b_n)\cdot(c_n,d_n)(a_n,b_n)^{-1}(c_n,d_n)^{-1}.$$

也就是 $g\in X$.

所以,$X=Y\otimes Z$. ▍

相应于多个群的外直积,也有多个子群的内直积概念.

定义 2 设 $A_1,\cdots,A_n$ 都是群 G 的不变子群,且对任意 $g\in G$,都有 $a_i\in A_i$, $i=1,2,\cdots,n$ 使

$$g=a_1a_2\cdots a_n,$$

而且表法唯一.那么,说 G 是 $A_1,\cdots,A_n$ 的**内直积**.

类似的,可以把命题 2 推广为

命题 5 设 $A_1,\cdots,A_n$ 是 G 的不变子群.那么,G 为 $A_1,\cdots,A_n$ 之内直积的充分必要条件是 $G=A_1A_2\cdots A_n$,且 G 之恒等元 e 表示成诸 A_i 元之乘积时,表法唯一. ▍

而把命题 3 推广成

命题 6 设 $A_1,\cdots,A_n$ 是 G 的不变子群.那么,G 为 $A_1,\cdots,A_n$ 之内直积的充分必要条件是 $G=A_1A_2\cdots,A_n$,且对每个 $i=1,2,\cdots,n$ 恒有 $A_i\cap(A_1\cdots A_{i-1}A_{i+1}\cdots A_n)=\{e\}$.

证明　与命题5相比较，我们要证明的是，在 $A_1,\cdots,A_n$ 均为 G 的不变子群，且 $G=A_1A_2\cdots A_n$ 的前提下，e 的表法唯一与对每个 $i=1,\cdots,n$，

$$A_i\cap(A_1\cdots A_{i-1}A_{i+1}\cdots A_n)=\{e\}$$

等价.

事实上，若 $g\in A_i\cap(A_1\cdots A_{i-1}A_{i+1}\cdots A_n)$，$g\neq e$. 由 A_i 都是 G 的不变子群，由§2例题，可以看出

$$A_iA_j=A_jA_i,$$

故 $g\in A_i\cap(A_{i-1}\cdots A_1A_n\cdots A_{i+1})$，设

$$g=b_{i-1}\cdots b_1b_n\cdots b_{i+1},\quad b_j\in A_j,$$

$$e=b_1^{-1}b_2^{-1}\cdots b_{i-1}^{-1}gb_{i+1}^{-1}\cdots b_n^{-1},$$

其中 $b_j^{-1}\in A_j$，$g\in A_i$，$g\neq e$，从而得到一个与

$$e=e\cdots e\cdots e \tag{6}$$

不同的表法.

反之，若 G 之恒等元 e 有如下表示

$$e=a_1a_2\cdots a_n$$

不同于(6). 则必有 k，$a_k\neq e$. 于是

$$a_k=a_{k-1}^{-1}\cdots a_1^{-1}a_n^{-1}\cdots a_{k+1}^{-1},$$

$$a_k\in A_k\cap(A_{k-1}\cdots A_1A_n\cdots A_{k+1}),$$

而诸 A_j 都是 G 的不变子群，

$$A_{k-1}\cdots A_1A_n\cdots A_{k+1}=A_1\cdots A_{k-1}A_{k+1}\cdots A_n,$$

所以 $A_k\cap(A_1\cdots A_{k-1}A_{k+1}\cdots A_n)\neq\{e\}$.　▌

关于内直积和外直积的关系，有

命题7　设 G 是其子群 $A_1,\cdots,A_n$ 的内直积. 则 G 同构于 $A_1,\cdots,A_n$ 的外直积 $A_1\otimes\cdots\otimes A_n$.

设 $H_1,\cdots,H_n$ 是群，那么，外直积

$$G=H_1\otimes\cdots\otimes H_n$$

是它的子群 $H_1',\cdots,H_n'$ 的内直积，$H_1'\approx H_1$，$\cdots$，$H_n'\approx H_n$． ▌

例题 3 若 G 是 $A_1,\cdots,A_n$ 的内直积，则 $G/A_1\approx A_2\cdots A_n$．

证明 对任意 $g\in G$，恒有 $a_i\in A_i$，$i=1,\cdots,n$，使

$$g=a_1a_2\cdots a_n,$$

且表法唯一．也就是说，$a_1,a_2,\cdots,a_n$ 都是由 g 唯一确定的，乘积 $a_2\cdots a_n$ 也是由 g 唯一确定的．

现规定 G 到 $A_2\cdots A_n$ 的映射 f，$f(g)=a_2\cdots a_n$，可以断言 f 是满同态映射．

首先，若 $g,h\in G$，

$$g=a_1\cdots a_n,\ a_i\in A_i;\quad h=b_1\cdots b_n,\ b_j\in A_j,$$

那么，由于 G 是诸 A_i 的直积，A_i 的元素与 A_j 的元素可换，故

$$gh=(a_1b_1)\cdots(a_nb_n).$$

由于表法唯一，$a_2b_2\cdots a_nb_n$ 是 gh 唯一确定的，从而

$$f(gh)=(a_2b_2)\cdots(a_nb_n)=(a_2\cdots a_n)(b_2\cdots b_n)=f(g)f(h),$$

f 为同态映射．

对任意 $x\in A_2\cdots A_n$，设 $x=d_2\cdots d_n$，$d_i\in A_i$，那么

$$f(ed_2\cdots d_n)=d_2\cdots d_n=x,$$

从而 f 是满的．

最后，计算 f 的核．若 $f(g)=e$，设 $g=a_1a_2\cdots a_n$，即应有

$$f(g)=a_2\cdots a_n=e.$$

由表法唯一性，必有 $a_2=e,\cdots,a_n=e$．也就是 $g=a_1\in A_1$．

反过来，对任意 $a_1\in A_1$，由 $a_1=a_1e\cdots e$ 知道

$$f(a_1)=e,\quad a_1\in \mathrm{Ker}(f).$$

所以，$\mathrm{Ker}(f)=A_1$．

由群同态基本定理得 $G/A_1\approx A_2\cdots A_n$． ▌

由于本节是选修的，所以，我们再做几个简单例题，而不给读者留习题．

例题 4 （参见习题四之题 3） 设

$$G=\{2^n5^m \mid m,n\in \mathbf{I}\},\ N=\{2^n \mid n\in \mathbf{I}\},\ K=\{5^m \mid m\in \mathbf{I}\}.$$

证明：G 是 N 和 K 的内直积.

证明 G 是交换群，N 和 K 都是其子群. 自然地是 G 的不变子群.

任取 $2^n5^m\in G$，则恒有 $2^n\cdot 5^m\in NK$.

同时，若有 $k,l\in \mathbf{I}$ 使 $2^k5^l=1$，我们分情况讨论，把这个等式写成

$$\begin{aligned}
2^k5^l&=1, &&\text{当 } k\geqslant 0,\ l\geqslant 0 \text{ 时},\\
2^k&=5^{-l}, &&\text{当 } k\geqslant 0,\ l\leqslant 0 \text{ 时},\\
2^{-k}&=5^l, &&\text{当 } k\leqslant 0,\ l\geqslant 0 \text{ 时},\\
2^{-k}5^{-l}&=1, &&\text{当 } k\leqslant 0,\ l\leqslant 0 \text{ 时}.
\end{aligned}$$

由于 2 和 5 都是素数，由整数分解的唯一性定理可推出，无论哪种情形，均有 $k=0,\ l=0$. 也就是说，G 中的恒等元 1 表成 N 中元与 K 中元之乘积时表法唯一.

所以，G 是 N 和 K 的内直积. ▌

例题 5（参看上节之例题 8） 用 $\mathbf{C}^\#$ 代表所有非零复数构成的乘法群，$\mathbf{R}+$ 代表正实数乘法群，N 代表所有模等于 1 的复数构成的 $\mathbf{C}^\#$ 的子群. 证明：$\mathbf{C}^\#$ 是 $\mathbf{R}^+$ 和 N 的直积.

证明 任取 $\alpha\in\mathbf{C}^\#$，α 可表成

$$\alpha=|\alpha|(\cos\theta+\mathrm{i}\sin\theta),\quad 0\leqslant\theta<2\pi,$$

其中 α 的模 $|\alpha|$ 是正实数，$\cos\theta+\mathrm{i}\sin\theta$ 模为 1，也就是

$$|\alpha|\in\mathbf{R}^+,\quad \cos\theta+\mathrm{i}\sin\theta\in N.$$

而且，由于 $\alpha\neq 0$，α 的模 $|\alpha|$ 和角 θ，$0\leqslant\theta<2\pi$ 都是由 α 唯一确定的. ▌

小　　结

本章的中心内容是商群概念和群同态基本定理. 为了学好这

些东西,我们已经做了大量的准备和铺垫,把"商"的思想逐步渗透给各位读者.

如果到现在为止,你对"商群"仍然觉得不甚了之(不是个别例子看不懂).甚至,对于某些商群的具体元素说不清楚.那么,你就不要只在§4兜圈子了.应该把前面整个这一阶段的学习总结一下了.

建议你的复习按下列步骤进行.

1. 重新学习第一章§3,弄清等价关系与分类问题的对应,分类决定商集,商集中元素如何表示或描述.

要彻底弄懂该节例11说明的问题.

例12中的$\mathbf{I}_{\sim n}$的元素$[0],\cdots,[n-1]$究竟代表了哪些集合,具体地写出几个来,比如$\mathbf{I}_{\sim 8}$,$\mathbf{I}_{\sim 13}$,$\mathbf{I}_{\sim 18}$.

2. 重新学习第一章§6,明确运算的定义与含义.非空集合S上的运算乃是$S\times S$到S的一个映射,给定$a,b\in S$要有唯一确定的元素ab与之对应.

这个"唯一确定"性在后面讨论商集上的运算时至关重要,它迫使我们规定商集上的运算时必须先证明"与代表元无关"等等,即定义的合理性.

特别地,对于例9之$\mathbf{I}_n$的元素形式及其上加法和乘法运算要了如指掌.

3. 复习第二章§1和§2,群及其子群.只看定义、例子,那些等价定义的推理证明可以跳过去.

4. 琢磨一下第二章§4命题5和命题6中给出的群$(\bar{\mathbf{I}},\boxplus)$.那是我们利用第二章一大段内容比较容易接受.新概念较少,有意插进来的一个"商群"的例子.关于定义合理性的议论绝非闲话.

5. 复习第二章§5关于左、右陪集与左右关系的内容.有了等价关系就有了分类,有了分类就有相应的商集.但群G对任意子群H的所有左陪集的集合能用G的运算定义成群吗?不能,关键是定义的合理性问题.

6. 再学第三章§2,引入不变子群概念.若 N 是 G 的不变子群,G/N 是 G 对 N 的所有左陪集(也是右陪集)构成的集合,规定

$$aN \ast bN = abN$$

就有意义了.

7. 对于第三章§4 给出的所有的商群的例子进行"加细",把每个群的元素尽量写得越多越细越好.如果自己能举些例子则更好.

这样单线串起来回顾一下,关于商群内容的学习会加深一步的.

关于群的同态,我们已经看到,同态核有举足轻重的作用.所以,一旦遇到群 G 到群 H 同态映射 f,首先要讨论 $\mathrm{Ker}(f)$,然后看 f 的像 $\mathrm{Img}(f)$,最后用同态基本定理即得

$$G/N \approx \mathrm{Img}(f), \quad N = \mathrm{Ker}(f).$$

当 $\mathrm{Ker}(f) = N$ 和 $\mathrm{Img}(f)$ 的结构清楚了,G 的结构也就相当清楚了.

种种要证明两群同构的问题最终都得把这个基本定理用上去.要想学过有关内容只能多实践(多做习题)多观察(看书).

复 习 题

1. 设 H, K 都是群 G 的子群,且 H 是 G 的不变子群.证明:$H \cap K$ 是 K 的不变子群.

2*. 设 H 是 G 的子群,对每个 $x \in G$ 得一子群 $H_x = \{xhx^{-1} \mid h \in H\}$.作它们的交集 $\bigcap_{x \in G} H_x = K$.证明:$K$ 是 G 的一个不变子群.

3. 设 H 是 G 的子群.证明:$N = \{x \in G \mid Hx = xH\}$ 是 G 的子群,而且 H 是 N 的不变子群.

4. 条件如上题,令 $C = \{y \in G \mid hy = yh$,对每个 $h \in H\}$,证明:C 是 N 的不变子群.

5. 问群$(\mathbf{I}_{13} - \{0^*\}, \cdot)$的子群 $H = \{1^*, 5^*, 8^*, 12^*\}$ 与群$(\mathbf{I}_{12} - \{0^*\}, \cdot)$的子群 $K = \{1^*, 5^*, 7^*, 11^*\}$ 能建立同构映射吗?

6. 令

$$i=\begin{pmatrix}0&-1&0&0\\1&0&0&0\\0&0&0&-1\\0&0&1&0\end{pmatrix},\quad j=\begin{pmatrix}0&0&-1&0\\0&0&0&1\\1&0&0&0\\0&-1&0&0\end{pmatrix},$$

$$k=\begin{pmatrix}0&0&0&-1\\0&0&-1&0\\0&1&0&0\\1&0&0&0\end{pmatrix},$$

而 e 代表 4 阶单位矩阵. 证明:$\{\pm e,\pm i,\pm j,\pm k\}$ 在矩阵乘法之下构成的群 G 同构于第二章 §2 习题之题 7 中给出的 8 个复 2 阶矩阵构成的乘法群. (它们都可以称为四元数群)

7. 设 G 是个有限群, f 是 G 的自同构, 同时, 当而且仅当 $x=e$ 时, 有 $f(x)=x$. 证明: 映射 $\sigma: x\to xf(x^{-1})$, $x\in G$ 是 G 上的可逆变换.

8. 看所有实的 2 阶矩阵构成的集合 $M_2(\mathbf{R})$ 的子集

$$G=\left\{\begin{pmatrix}a&b\\-b&a\end{pmatrix}\,\middle|\,a,b\in\mathbf{R}\right\}.$$

证明: G 在矩阵加法之下构成的群 $(G,+)$ 同构于所有复数构成的加法群 $(\mathbf{C},+)$. 再证明: G 中所有非零矩阵的集合 $G^{\#}$ 在矩阵乘法之下构成的群 $(G^{*},\cdot)$ 同构于所有非零复数的集合 $\mathbf{C}^{\#}$ 在数的乘法之下构成的群 $(\mathbf{C}^{\#},\cdot)$.

9. 设 G 是个交换群, n 是个固定的正整数, σ 是 G 到 G 的映射

$$\sigma: x\to x^n,\quad x\in G.$$

证明: σ 是群同态, 并给出 $\mathrm{Ker}(\sigma)$.

10. 设 G 是所有形如

$$\begin{pmatrix}a&b\\0&d\end{pmatrix},\quad a\neq0,\ d\neq0$$

的实的 2 阶矩阵构成的乘法群. K 是所有形如

$$\begin{pmatrix}1&b\\0&d\end{pmatrix},\quad d\neq0$$

的实 2 阶矩阵构成的乘法群. 证明: K 是 G 的不变子群, 给出商群 G/K.

11*. 设 $(\mathbf{Q},+)$ 是有理数加解, $(\mathbf{I},+)$ 是整数加解. 求出商群 $\mathbf{Q}/\mathbf{I}$ 中所有周期有限的元素.

第四章 环与理想

前两章讨论的群是个仅有一个二元运算的代数系统.本书的后几章将要学习同时具有两种二元运算的代数系统.

当然,一个集合上的两种二元运算各有各的规律,这就需要读者首先掌握好有一种二元运算的系统的研究方法,特别是群论方法.

同时,一个集合上的两种二元运算配合在一起形成一个整体,就需要密切注意这两种运算的联系,而不是讨论那类两种二元运算“不搭边”的各自独立无关系统.

近世代数学中常见的有两个二元运算的代数系统有结合环、Lie环、Jordan环、格和Boole代数,等等,其中结合环背景最为广泛,研究的历史最长,已成为近世代数学的最基本的学习内容之一.

§1 环的定义

定义1 设集合 R 上有两种二元运算,一个叫加法,记为 $+$;一个叫乘法,记为 $\cdot$,且

(1) $(R,+)$是个交换群;

(2) 乘法 $\cdot$ 在 R 上是结合的;

(3) 对任意 $a,b,c\in R$,都有

$$a\cdot(b+c)=a\cdot b+a\cdot c,\quad (b+c)\cdot a=b\cdot a+c\cdot a$$

则说$(R,+,\cdot)$是个**结合环**,简单地,说它是个**环**.

在不致引起混淆的情形下，也可说 R 是个环，把 $a\cdot b$ 写成 ab 而省去乘号. 定义中的(3)通常称为**分配律**，环中运算，在无括号时，如同数一样，仍然是先乘后加.

例 1 整数集 **I** 在通常数的加法、数的乘法之下是个环.

有理数集、实数集、复数集、偶数集在相应的运算之下，亦分别是个环.

例 2 设

$$F=\{f\mid f:\mathbf{R}\to\mathbf{R}\}.$$

即，F 是 **R** 到 **R** 的所有映射的集合，也就是定义在 $(-\infty,+\infty)$ 上所有实函数的集合. 规定，对任意 $f,g\in F$，

$$f\#g:x\to f(x)+g(x),\quad x\in\mathbf{R},$$

$$f\odot g:x\to f(x)g(x),\quad x\in\mathbf{R},$$

则 $(F,\#,\odot)$ 是个环.

首先，由第二章习题一之题 5 知道 $(F,\#)$ 是个交换群.

其次，要证明 $\odot$ 运算满足结合律，也就是要证明，对任意 $f,g,h\in F$，有

$$(f\odot g)\odot h=f\odot(g\odot h).$$

而要证明上面这样一个映射的等式，据映射相等的定义，我们必须而且只需证明，等式两端的两个映射对 **R** 的每个实数 x 作用相同. 事实上，对任意 $x\in\mathbf{R}$，我们有

$$\begin{aligned}
&[(f\odot g)\odot h](x)\\
&\quad=(f\odot g)(x)h(x) &&(\text{运算}\odot\text{的定义})\\
&\quad=(f(x)g(x))h(x) &&(\text{运算}\odot\text{的定义})\\
&\quad=f(x)[g(x)h(x)] &&(\text{实数乘法结合律})\\
&\quad=f(x)[(g\odot h)(x)] &&(\text{运算}\odot\text{的定义})\\
&\quad=[f\odot(g\odot h)](x). &&(\text{运算}\odot\text{的定义})
\end{aligned}$$

所以，$(f\odot g)\odot h=f\odot(g\odot h)$.

最后，验证 $\#$ 和 $\odot$ 满足分配律，对任意 $g,h,f\in F$ 及任意 $x\in\mathbf{R}$，有

$$[(g \# h)\odot f](x)$$
$$= (g \# h)(x)f(x) \qquad \text{(运算}\odot\text{的定义)}$$
$$= [g(x)+h(x)]f(x) \qquad \text{(运算}\#\text{的定义)}$$
$$= g(x)f(x)+h(x)f(x) \qquad \text{(实数加乘适合分配律)}$$
$$= (g\odot f)(x)+(h\odot f)(x) \qquad \text{(运算}\odot\text{的定义)}$$
$$= [(g\odot f)\#(h\odot f)](x). \qquad \text{(运算}\odot\text{的定义)}$$

所以,$(g \# h)\odot f=(g\odot f)\#(h\odot f)$.同理可证,

$$f\odot(g \# h)=(f\odot g)\#(f\odot h).$$

例 3 设 n 是个正整数,

$$\mathbf{I}_n=\{0^*,1^*,\cdots,(n-1)^*\}.$$

在第一章§6 我们已经定义了 $\mathbf{I}_n$ 上的加法和乘法.在第二章中,证明了$(\mathbf{I}_n,+)$是个加法群.

现证 $\mathbf{I}_n$ 上乘法满足结合律(先复习一下第一章§6 之例题 2).任取 $i^*,j^*,k^*\in\mathbf{I}_n$,设 $i^*\times j^*=l^*$, $l^*\times k^*=m^*$,即有整数 x,y 使得

$$i\times j=xn+l,\ 0\leqslant l<n;\quad l\times k=yn+m,\ 0\leqslant m<n.$$

同时又设 $j^*\times k^*=s^*$, $i^*\times s^*=t^*$,即有整数 u,v 使得

$$j\times k=un+s,\ 0\leqslant s<n;\quad i\times s=vn+t,\ 0\leqslant t<n.$$

那么,由于

$$i\times(j\times k)=iun+is=iun+vn+t,$$
$$(i\times j)\times k=kxn+kl=kxn+yn+m,$$

而$0\leqslant m,t<n$,据第一章§6 引理知,$m=t$,进而知 $m^*=t^*$,也就是

$$(i^*\times j^*)\times k^*=i^*\times(j^*\times k^*).$$

再证 $\mathbf{I}_n$ 上加法和乘法适合分配律.任取 $i^*,j^*,k^*\in\mathbf{I}_n$,设

$$j^*+k^*=l^*,\quad l^*\times i^*=m^*,$$

即有整数 s,t 使得

$$j+k=ns+l,\ 0\leqslant l<n;\quad li=nt+m,\ 0\leqslant m<n.$$

再设 $j^*\times i^*=p^*$, $k^*\times i^*=q^*$,即有整数

$$j\times i=xn+p,\ 0\leqslant p<n;\quad k\times i=yn+q,\ 0\leqslant q<n.$$

于是,由整数的分配律成立,即$(j+k)i=ji+ki$得到

$$(j+k)i=nsi+nt+m,\quad 0\leqslant m<n,$$

$$ji+ki=nx+ny+p+q.$$

从而必有整数 u 使

$$p+q=un+m,\quad 0\leqslant m<n;$$

即 $p^*+q^*=m^*$,也就是

$$(j^*+k^*)i^*=j^*i^*+k^*i^*.$$

另一侧分配律不证自明.

例 4 设 0 是加法群$(G,+)$的零元素.规定 G 上的二元运算 $*$,使任意 $a,b\in G$ 恒对应 0,即

$$a*b=0,\quad 对任意\ a,b\in G.$$

那么,$(G,+,*)$是个环.

例 5 由于 4 阶对称群 S_4 的子群

$$R=\{e,(1\ 2),(3\ 4),(1\ 2)(3\ 4)\}$$

是个交换群,我们把 e 记为 0,把(1 2),(3 4)和(1 2)(3 4)分别记为 a,b,c,于是其运算表是

#	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

再定义 R 上一个二元运算 $*$,它的运算表是

$*$	0	a	b	c
0	0	0	0	0
a	0	a	0	a
b	0	b	0	b
c	0	c	0	c

首先,对任意 $x,y\in R$,有

$(x*y)*0=x*(y*0)=0^*$, (0 右乘任何元均得 0)

$(x*y)*b=x*(y*b)$, (b 右乘任何元亦得 0)

$(x*y)*a=x*y=x*(y*a)$, (a 右乘任何元均不变该元)

$(x*y)*c=x*(y*c)$. (c 右乘任何元亦不变该元)

这说明,对任意 $x,y,z\in R$ 恒有

$$(x*y)*z=x*(y*z).$$

即 $*$ 满足结合律.

又,对任意 $x,y\in R$,

$(x\#y)*0=(x*0)\#(y*0)$, (0 右乘任何元得 0)

$(x\#y)*b=(x*b)\#(y*b)$, (b 右乘任何元得 0)

$(x\#y)*a=x\#y=(x*a)\#(y*a)$, ($a$ 右乘不变该元)

$(x\#y)*c=(x*c)\#(y*c)$. (c 右乘不变该元)

再则,对任意 $x,y,z\in R$,只要其中之一为 0,则必有

$$x*(y\#z)=(x*y)\#(x*z).$$

同时,若 $y=z$,亦必有 $x*(y\#y)=0=(x*y)\#(x*y)$.

取 $x=a$, $y\neq z$,很容易看出,只剩如下 3 种情形需要验证,注意乘法表和加法表,有

$a*(a\#b)=a*c=a=a\#0=(a*a)\#(a*b)$,

$a*(a\#c)=a*b=0=(a*a)\#(a*c)$,

$a*(b\#c)=a*a=a=(a*b)\#(a*c)$.

取 $y=b,c$ 又各有 3 种情形需要验证,而道理是完全一样的.所以,对任意 $x,y,z\in R$,有 $x*(y\#z)=(x*y)\#(x*z)$.

总之,$(R,\#,*)$满足乘法 $*$ 结合律和乘法与加法的分配律,它是个环.

遇到类似的代数系统时,验算各种算律一定要细心,既要简明又不可漏掉任意一个情形.

例 6 设 $M_{n\times n}$ 代表所有实的 n 阶方阵的集合.在通常的矩阵加法 $+$ 和乘法 $\cdot$ 之下,即

$$(a_{ij})+(b_{ij})=(a_{ij}+b_{ij}),\quad (a_{ij})\cdot(b_{ij})=(c_{ij}),$$

其中 $c_{ij}=\sum_{k=1}^{n}a_{ik}b_{kj}$,那么$(M_{n\times n},+,\cdot)$是个环.

这是环理论中最重要的一种类型的环.

例题 1 设$(G,+)$是个交换群,用 E 代表所有 G 到 G 的同态映射的集合.规定,对任意 $\sigma,\tau\in E$,

$$\sigma\#\tau: x\to\sigma(x)+\tau(x),\quad x\in G,$$

$$\sigma\circ\tau: x\to\sigma(\tau(x)),\quad x\in G,$$

则得到 E 上两个运算 # 和$\circ$. 证明:$(E,\#,\circ)$是个环.

证明 若 $\sigma,\tau\in E$,即 σ 和 τ 都是 G 到 G 的同态映射,那么复合映射 $\sigma\circ\tau$ 亦为 G 到 G 的同态映射,$\sigma\circ\tau\in E$.

要验证上面确定的 G 到 G 的映射 $\sigma\#\tau$ 是个同态映射,我们任取 $x,y\in G$,必有

$$\begin{aligned}&(\sigma\#\tau)(x+y)\\&\quad=\sigma(x+y)+\tau(x+y) &&(\#\text{的定义})\\&\quad=\sigma(x)+\sigma(y)+\tau(x)+\tau(y) &&(\sigma\text{和}\tau\text{是同态})\\&\quad=\sigma(x)+\tau(x)+\sigma(y)+\tau(y) &&(G\text{之加法可换})\\&\quad=(\sigma\#\tau)(x)+(\sigma\#\tau)(y). &&(\#\text{的定义})\end{aligned}$$

所以,$\sigma\#\tau$ 是个同态映射,$\sigma\#\tau\in E$. # 是 E 上的运算.

不难证明 # 满足交换律和结合律,零同态 0^* 是 E 的加法零元素,对任意 $\sigma\in E$,

$$-\sigma: x\to-\sigma(x),\quad x\in G$$

是 σ 的负元,从而$(E,\#)$是个交换群.

映射复合$\circ$满足结合律.

任取 $\sigma,\tau,\rho\in E$ 及 $x\in G$,有

$$\begin{aligned}&[(\sigma\#\tau)\circ\rho](x)\\&\quad=(\sigma\#\tau)[\rho(x)] &&(\text{复合的定义})\\&\quad=\sigma[\rho(x)]+\tau[\rho(x)] &&(\#\text{的定义})\\&\quad=(\sigma\circ\rho)(x)+(\tau\circ\rho)(x) &&(\circ\text{的定义})\end{aligned}$$

$$=[(\sigma\circ\rho)\#(\tau\circ\rho)](x).\qquad (\#\text{的定义})$$

所以，$(\sigma\#\tau)\circ\rho=(\sigma\circ\rho)\#(\tau\circ\rho)$.

另一方面，

$$
\begin{aligned}
&[\rho\circ(\sigma\#\tau)](x)\\
&=\rho((\sigma\#\tau)(x)) && (\circ\text{的定义})\\
&=\rho(\sigma(x)+\tau(x)) && (\#\text{的定义})\\
&=\rho[\sigma(x)]+\rho[\tau(x)] && (\rho\text{ 是同态映射})\\
&=(\rho\circ\sigma)(x)+(\rho\circ\tau)(x) && (\circ\text{的定义})\\
&=[(\rho\circ\sigma)\#(\rho\circ\tau)](x). && (\#\text{的定义})
\end{aligned}
$$

所以，$\rho\circ(\sigma\#\tau)=(\rho\circ\sigma)\#(\rho\circ\tau)$. ∎

这里，应该注意到，该题证明两个分配律时用到的理由不尽相同，后边的用到了映射 ρ 的同态性，而前者只用到 $\#$ 和 $\circ$ 的定义．这个例子告诉我们，在环的定义的公理中，两个分配律是独立的．并不是在任何体系中，只要证明了它满足一侧的分配律则另一侧分配律必同理可证．

例题 2．设 $(G,+)$ 是个加法群，用 F 代表所有 G 到 G 的映射的集合．规定，对意 $\sigma,\tau\in F$，

$$\sigma\#\tau: x\to\sigma(x)+\tau(x),\quad x\in G,$$

$$\sigma\circ\tau: x\to\sigma(\tau(x)),\quad x\in G.$$

则 $\#$ 和 $\circ$ 都是 F 上的二元运算，问，$(F,\#,\circ)$ 是个环吗？

分析　对任意 $\sigma,\tau\in F$，$\sigma\#\tau$ 和 $\sigma\circ\tau$ 都是确定的 G 到 G 的映射，即 $\sigma\#\tau\in F$，$\sigma\circ\tau\in F$，从而 $\#$ 和 $\circ$ 是 F 的运算．

仔细验证，不难发现，$(F,\#)$ 是个加法群，运算 $\circ$ 是可结合的．问题出在分配律上．为此，只需举一反例即可．

证明　设 $G=\mathbf{I}_2=\{0^*,1^*\}$，$\sigma(0^*)=1^*$，$\sigma(1^*)=1^*$．于是

$$[\sigma\circ(\sigma\#\sigma)](1^*)=1^*,\quad [(\sigma\circ\sigma)\#(\sigma\circ\sigma)](1^*)=0^*.$$

从而 $\#$ 和 $\circ$ 不满足分配律． ∎

例题 3　设 S 是个集合，R 是 S 的所有子集构成的集合．规

定，任意 $A,B\subseteq S$，

$$A\# B=\{x\in S\mid x\in A\cup B \text{ 且 } x\notin A\cap B\},$$

$$A\cdot B=\{x\in S\mid x\in A\cap B\}.$$

证明：$(R,\#,\cdot)$是个环。

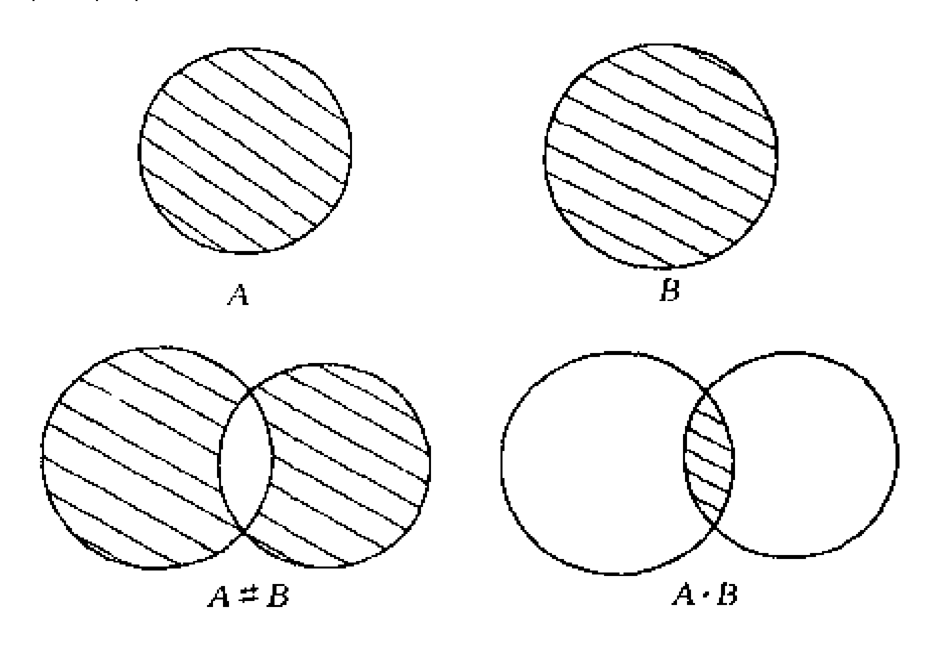


图 4－1

证明 上图之阴影部分已用字母标出，$A\# B$ 乃是 $A\cup B$ 去掉 $A\cap B$ 而成.

首先，对任意 $A,B,C\in R$，即 $A,B,C\subseteq S$，容易看出 $(A\# B)\# C$ 和 $A\#(B\# C)$ 相等，如图 4－2，它们都是图中之阴影部分.

其次，对任意 $A\subseteq S$，都有 $A\#\varnothing=A$，即空集$\varnothing$是 R 的零元素.

再次，对任意 $A\in R$，即 $A\subseteq S$，有 $A\# A=\varnothing$. 所以 A 是 A 的负元.

所以，$(R,\#)$是个群，而且是可换的.

进而，R 上的交运算·是可结合的.

最后，来验证 R 上#和·适合分配律. 对任意 $A,B,C\in R$. 设 $x\in A\cdot(B\# C)$，即

$$x\in A,\quad x\in B\cup C,\quad x\notin B\cap C.$$

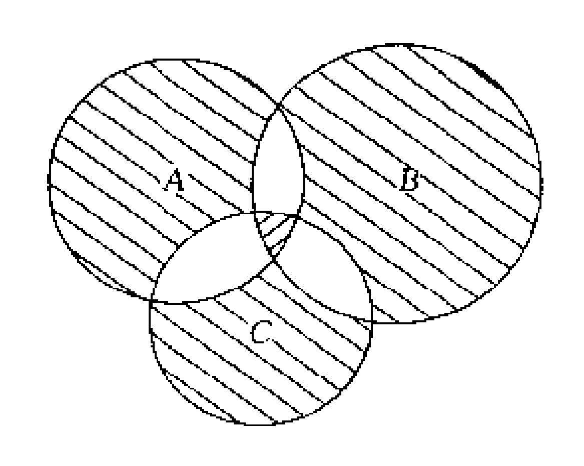


图 4－2

若 $x\in B$，$x\notin C$，则 $x\in A\cap B$ 但 $x\notin A\cap C$，从而

$$x\in(A\cap B)\#(A\cap C)=(A\cdot B)\#(A\cdot C);$$

若 $x\in C$，$x\notin B$，则 $x\in A\cap C$ 但 $x\notin A\cap B$，从而亦有 $x\in(A\cap B)\#(A\cap C)$. 即

$$A\cdot(B\# C)\subseteq(A\cap B)\#(A\cap C).$$

反之，设 $x\in(A\cap B)\#(A\cap C)$，那么或者 $x\in A\cap B$ 但 $x\notin A\cap C$，或者 $x\in A\cap C$ 但 $x\notin A\cap B$. 于是必有

$$x\in A,\quad x\in B,\quad x\notin C,$$

或者

$$x\in A,\quad x\in C,\quad x\notin B,$$

也就是 $x\in A\cap(B\# C)=A\cdot(B\# C)$. 所以，

$$A\cdot(B\# C)=(A\cdot B)\#(A\cdot C).$$

另一侧之分配律也是容易证明的. ▌

命题 1 设 $(R,+,\cdot)$ 是个环，0 是 $(R,+)$ 的零元素，$-a$ 代表 $(R,+)$ 中 a 的负元素. 那么，对任意 $a,b,c\in R$，有

(1) $0\cdot a=a\cdot 0=0$;

(2) $a\cdot(-b)=(-a)\cdot b=-a\cdot b$;

(3) $(-a)\cdot(-b)=a\cdot b$;

(4) $a\cdot(b-c)=a\cdot b-a\cdot b,(a-b)\cdot c=a\cdot c-b\cdot c$.

证明 对任意 $a\in R$，有

$$0\cdot a=(0+0)\cdot a,\qquad (0\text{ 是零元})$$

$$0\cdot a=0\cdot a+0\cdot a,\qquad \text{(分配律)}$$
$$0=0\cdot a.\qquad \text{(加法消去律)}$$
对任意 $a,b\in R$，有
$$a\cdot(-b)+a\cdot b=a(b+(-b)),\qquad \text{(分配律)}$$
$$a\cdot(-b)+a\cdot b=0,\qquad \text{(上面证过)}$$
这说明 $a\cdot(-b)$ 是 $a\cdot b$ 的负元，由负元的唯一性知道 $a\cdot(-b)=-(a\cdot b)$. 同理，$(-a)\cdot b=-a\cdot b$.

由于 $(-a)\cdot(-b)=-[a\cdot(-b)]=-[-a\cdot b]$，而任何元素的负元的负元恰为该元自己，故 $(-a)\cdot(-b)=a\cdot b$.

由于 $b-c$ 即 $b+(-c)$，故
$$a\cdot(b-c)=a\cdot b+a\cdot(-c)=a\cdot b+(-a\cdot c).$$
也就是 $a\cdot(b-c)=a\cdot b-a\cdot c$. 同理，$(a-b)\cdot c=a\cdot c-b\cdot c$. ▌

这个命题证明了环 R 的零元素 0 与任何元素 a 相乘均为 0. 但是，反过来，由环的定义不能保障 $a\neq 0$ 且 $b\neq 0$ 则必有 $a\cdot b\neq 0$. 这我们可以从例 4、例 6 和例题 2 看出来.

定义 2 设 $(R,+,\cdot)$ 是个环，如果 R 的乘法有单位元 e（即恒等元），则说 R 是个**有单位元环**，或称**有 1 环**. 称 e 为 R 的**单位元**（或恒等元）；对于环 R 的元素 a，若有 $b\neq 0$ 以及 $c\neq 0$ 使 $ab=0$ 以及 $ca=0$，则说 a 是 R 的一个**零因子**；如果环 R 不含非零的零因子，则称 R 为**无零因子环**；如果环 R 的乘法是可换的，则说 R 是个**交换环**；有 1 的交换的无零因子环称为**整环**或**整区**.

例如，整数环、有理数环、实数环都是整环，但偶数环不是整环，它没有一个元素是乘法单位元.

例题 4 环 $(\mathbf{I}_n,+,\times)$ 是整环的充分必要条件是 n 为素数.

证明 我们已经知道 1^* 是 $\mathbf{I}_n$ 的恒等元，乘法·可交换.

当 n 为素数时，若 $i^*\neq 0^*$，$j^*\neq 0^*$，设
$$i\times j=tn+r,\quad 0\leqslant r<n,$$
则 $r\neq 0$，否则 n 必整除 i 或整除 j. 所以
$$i^*\times j^*=r^*\neq 0^*.$$

反之,若 n 不为素数,

$$n = st, \quad 1 < s < n, \; 1 < t < n,$$

则 $s^* \times t^* = 0^*$, I_n 有非零的零因子. ▌

命题 2 如果$(R, +, \cdot)$是个整区,那么 R 的乘法满足消去律;即 $a, b, c \in R$, $a \neq 0$.则 $a \cdot b = a \cdot c$ 蕴涵 $b = c$.

事实上,若 $a \cdot b = a \cdot c$,则

$$0 = a \cdot b - a \cdot c = a(b - c).$$

而 $a \neq 0$,R 无非零的零因子,故必有 $b - c = 0$,也就是 $b = c$. ▌

例题 5 环$(R, +, \cdot)$中任何元素 a 恒有$a \cdot a = a$,则 R 必为交换环.

证明 任取 $a, b \in R$.据题设,有

$$(a + b) \cdot (a + b) = a + b.$$

但是,由命题 1 知

$$(a + b) \cdot (a + b) = a \cdot a + a \cdot b + b \cdot a + b \cdot b,$$

从而知

$$a + b = a \cdot a + a \cdot b + b \cdot a + b \cdot b.$$

再由 $a \cdot a = a$, $b \cdot b = b$ 及加法消去律可得

$$a \cdot b + b \cdot a = 0. \tag{1}$$

因为(1)对任意 $a, b \in R$ 都成立,特别地取 $a = b$,则有

$$a \cdot a + a \cdot a = a + a = 0,$$

即对任意 $a \in R$ 都有$a = -a$.于是,(1)式就变成

$$a \cdot b = -b \cdot a = b \cdot a,$$

这意味着 R 是可换环. ▌

由于一个环$(R, +, \cdot)$即是一个加法群$(R, +)$又是一个有乘法的代数系统,所以,前两章中关于有一个二元运算的系统、加法群所惯用的写法即可直接使用而毋需再做解释.

例如,k 是正整数,

$$a^k = aa\cdots a, \quad k \text{ 个 } a \text{ 相乘},$$

$$ka = a + \cdots + a, \quad k \text{ 个 } a \text{ 相加},$$

当 k 为负整数时，

$$ka=(-a)+\cdots+(-a),\quad k\text{ 个 }-a\text{ 相加}.$$

命题 3 如果环$(R,+,\cdot)$有乘法恒等元，设为 e，那么对任意 $n\in \mathbf{I}$, $a\in R$，有 $na=(ne)a$.

证明 当 $n=0$ 时，$0a=0$, $0e=0$，当然有 $0a=(0e)a$.

当 $n>0$ 时，

$$na=a+a+\cdots+a,\quad n\text{ 个 }a\text{ 相加},$$

$$(ne)a=(e+e+\cdots+e)a,\quad n\text{ 个 }e\text{ 相加}.$$

用分配律，立得

$$(ne)a=ea+\cdots+ea=a+\cdots+a=na.$$

当 $n<0$ 时，$m=-n>0$，且

$$na=(-m)a=m(-a),$$

前已证明，

$$m(-a)=(me)(-a),$$

用命题 2 得$(me)(-a)=(-(me))a$. 在群论中已熟知 $-(me)=(-m)e$. 所以，

$$na=m(-a)=(me)(-a)=(-(me))a=(ne)a. \quad \blacksquare$$

给定一个交换环 R，把 R 的 $n\times n$ 个元素排成一个正方表

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix},\quad a_{ij}\in R,$$

即称为是 R 上的一个 $n\times n$ 矩阵或 n 阶方阵，a_{ij} 称为 A 的 i 行 j 列元素.

规定

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}+\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}$$

$$
=\begin{pmatrix} a_{11}+b_{11} & \cdots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & \cdots & a_{2n}+b_{2n} \\ \vdots & & \vdots \\ a_{n1}+b_{n1} & \cdots & a_{nn}+b_{nn} \end{pmatrix},
$$

$$
\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}
$$

$$
=\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix},
$$

其中

$$
c_{ij}=\sum_{k=1}^{n} a_{ik}b_{kj}, \quad 1\leqslant i,j\leqslant n.
$$

仿照《高等代数》中对数字矩阵的讨论,容易验证,R 上所有 n 阶方阵的集合 $M_{n\times n}(R)$在上述运算之下构成一个环,称为 R 上 n **阶全阵环**.

当 R 有单位元 e 时,矩阵

$$
\begin{pmatrix} e & 0 & \cdots & 0 \\ 0 & e & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & e \end{pmatrix}
$$

即为 $M_{n\times m}(R)$的单位元.即使 R 是可换的,当 $n>1$ 时,$M_{n\times n}(R)$却可能是非交换.当 R 是整区时,$M_{n\times n}(R)$却可能有非零的零因子.

矩阵是环论讨论的主要背景之一,在处理特殊问题考虑反例时,矩阵环是首选对象.

定义 3 设 R 是个有单位元 1 的环. R 的元素 a 称为 R 的一个**单位**,如果有 $b\in R$ 使 $ab=ba=1$.

学过《线性代数》的人都知道,数域上的 n 阶方阵不为零因子则必为可逆矩阵. 用我们这里的术语来说,就是,数域 F 上的 n 阶全阵环 $M_{n\times n}(F)$ 中,某元素不为零因子则必为单位.

但是,此事实不能照搬到任意交换环 R 的情形. 例如,整数环 $\mathbf{I}$ 上 2 阶全阵环 $M_{2\times 2}(\mathbf{I})$ 中,矩阵

$$T=\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}$$

不为零因子. 因为,对任意 $A\in M_{2\times 2}(\mathbf{I})$,设

$$A=\begin{pmatrix}a & b\\ c & d\end{pmatrix},\quad a,b,c,d\in\mathbf{I},$$

恒有

$$\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}=\begin{pmatrix}2a & 2b\\ 2c & 2d\end{pmatrix}.$$

要

$$\begin{pmatrix}2a & 2b\\ 2c & 2d\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},$$

必须有 $2a=1$, $2d=1$,但 $a,d\in\mathbf{I}$,这是办不到的事情. 故矩阵 T 不是单位.

同时,当 $A\neq 0$ 时,即 a,b,c,d 不全为 0 时,$2a,2b,2c,2d$ 亦不全为 0;也就是

$$TA=AT\neq 0,$$

这说明 T 不为零因子.

单位元是个单位,但不要把单位错当成单位元,这一点,看书时要特别加以注意.

习 题 一

1. 用 E 代表偶数集,+ 是数的加法. 规定,任意 $m,n\in E$, $m\circ n=$

$\frac{1}{2}mn$. 证明：$(E,+,\circ)$是个环.

2. 环$(R,+,\cdot)$为交换环的充分必要条件是，对任意$a,b\in R$都有

$$a^2-b^2=(a+b)(a-b).$$

3. 设$(R,+,\cdot)$是个环，$a,b,c\in R$. 证明：$(a-b)+(b-c)=a-c$.

4. 设环$(R,+,\cdot)$为无零因子环，$e\in R$. 如果$e\cdot e=e$，那么e是R的恒等元.

5. 设$(R,+)$是个交换群. 规定，对任意$a,b\in R$，$a\cdot b=0$. 证明：$(R,+,\cdot)$是个环.

6. 证明：含1的交换环满足乘法消去律即必为整环.

7. 证明：任意一个含5个元素的环都是交换的.

§2 子环和理想

定义1 设$(R,+,\cdot)$是个环，S是R的一个非空子集. 如果$+$和$\cdot$也是S的运算，且$(S,+,\cdot)$也是个环，则说$(S,+,\cdot)$是$(R,+,\cdot)$的一个**子环**. 当所指运算不会混淆时，可简单地说S是R的子环.

例1 上节例1中，偶数环是有理数环的子环；偶数环、有理数环都是实数环的子环.

例2 上节例2中，用C代表所有连续的实函数的集合. F上的运算#和$\odot$使任意$f,g\in C$对应.

$$f\#g: x\to f(x)+g(x),\quad x\in\mathbf{R},$$
$$f\odot g: x\to f(x)g(x),\quad x\in\mathbf{R}.$$

由于$f\#g$和$f\odot g$仍为连续函数，故#和$\odot$也是C上的运算. 而且$(C,\#)$是交换群.

至于#和$\odot$满足环定义对运算律的要求是很容易说明的. 所以$(C,\#,\odot)$是$(F,\#,\odot)$的一个**子环**.

例3 设$M_{n\times n}$是所有n阶实方阵作成的环(上节之例4). 那么

$$E_{n\times n}=\{(a_{ij})\in M_{n\times n}\mid a_{ij}\text{为偶数}\}$$

是 $M_{n\times n}$ 的一个子环. 同时

$$S=\{(a_{ij})\in M_{n\times n}\mid i<j\text{ 时 }a_{ij}=0\}$$

也是 $M_{n\times n}$ 的一个子环. S 中的矩阵即所谓下三角矩阵, 对角线以上的元素恒为 0, 即有形式

$$\begin{pmatrix} a_{11} & 0 & 0 & \cdots & 0 \\ a_{21} & a_{22} & 0 & \cdots & 0 \\ a_{31} & a_{32} & a_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{pmatrix}.$$

在《高等代数》中, 我们知道, 下三角矩阵之和、差仍为下三角矩阵, $(S,+)$ 是个交换群, 同时两个下三角之积仍为下三角矩阵.

同理, 所有形如

$$\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}_{n\times n}$$

的实距阵, A 是 m 阶方阵, $m\leqslant n$, 也作成 $M_{n\times n}$ 的一子环.

所有形如

$$\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ a_{n1} & 0 & \cdots & 0 \end{pmatrix}$$

的实矩阵也作为 $M_{n\times n}$ 的一个子环, 记为 M_1.

命题 1 设 $(R,+,\cdot)$ 是个环, S 是 R 的非空子集. 那么, S 是 R 的子环的充分必要条件是

(1) 对任意 $a,b\in S$, 有 $a+b\in S$;

(2) 对任意 $a\in S$, 有 $-a\in S$;

(3) 对任意 $a,b\in S$, 有 $a\cdot b\in S$.

证明 若 $(S,+,\cdot)$ 是 $(R,+,\cdot)$ 子环, 则群 $(S,+)$ 是 $(R,+)$

的子群. 由第二章§2知道 S 必有满足(1)和(2).

R 的乘法也是 S 上乘法,故 S 满足(3).

反过来,如果 S 满足(1)和(2),则 R 的加法必然是 S 上运算,且 $(S,+)$ 为交换群. 而条件(3)即保证了 R 的乘法也是 S 上的运算. 自然地 S 上乘法满足结合律.

由于 S 上运算乃是 R 的运算派生出来,它们当然还满足分配律.

所以, S 是 R 的子环. ▌

例 4 在实数环 $\mathbf{R}$ 中,所有形如

$$a+b\sqrt{2},\quad a,b \text{ 为整数}$$

的数构成 $\mathbf{R}$ 的一个子环.

记所有这种形式的实数的集合为 S.

对任意 $x=a+b\sqrt{2}\in S$,有

$$-x=-(a+b\sqrt{2})=(-a)+(-b)\sqrt{2},$$

$-a$ 和 $-b$ 仍然为整数,从而 $-x\in S$.

对任意 $x=a+b\sqrt{2}$, $y=c+d\sqrt{2}\in S$,有

$$x+y=(a+c)+(b+d)\sqrt{2},$$

而 $a+c$ 和 $b+d$ 亦为整数,故 $x+y\in S$.

最后,对任意 $x=a+b\sqrt{2}$, $y=c+d\sqrt{2}\in S$,有

$$xy=(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2},$$

其中 $ac+2bd$ 和 $ad+bc$ 都是整数. 所以 $xy\in S$.

总结之, S 为 R 的子环.

例题 1 S 是所有形如 $a/2^n$ 的有理数构成的集合,其中 a 和 n 是整数. 证明: S 是有理数环的子环.

证明 对任意 $x=a/2^n$, $y=b/2^m\in S$,有

$$a/2^n+b/2^m=(a2^m+b2^n)/2^{m+n}\in S,$$

$$(a/2^n)\cdot(b/2^m)=ab/2^{m+n}\in S,$$

$$-(a/2^n)=(-a)/2^n\in S.$$

故 S 为有理数环的子环. ∎

例题 2 在复数域上所有 2 阶方阵构成的环 R 中,所有形如

$$x=\begin{pmatrix} a+b\sqrt{-1} & c+d\sqrt{-1} \\ -c+d\sqrt{-1} & a-b\sqrt{-1} \end{pmatrix},\quad a,b,c,d \text{ 为实数},$$

的矩阵的集合 S 是 R 的一个子环.

证明 令

$$e=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\quad i=\begin{pmatrix} \sqrt{-1} & \\ & -\sqrt{-1} \end{pmatrix},\quad j=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$k=\begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}.$$

则 S 中的任意元 x 恒可写成

$$x=ae+bi+cj+dk.$$

于是,对任意 $x,y\in S$,很容易看出,$x+y$ 和 $-x$ 属于 S.

同时,研究 e,i,j,k 的乘法表,

	e	i	j	k
e	e	i	j	k
i	i	$-e$	k	$-j$
j	j	$-k$	$-e$	i
k	k	j	$-i$	$-e$

即知,若 $x,y\in S$,则矩阵 xy 亦为矩阵 e,i,j,k 用实数相乘后相加而得,即 $xy\in S$.

故 S 是 R 的子环. ∎

读者只要仔细对照我们在群理论中的讨论,很容易看出命题 1 的(1),(2)两款等价于$(S,+)$是$(R,+)$的加法子群. 所以,有

命题 2 设$(R,+,\cdot)$是个环,S 是 R 的非空子集. 那么,S 是 R 的子环的充分必要条件是

(1) $(S,+)$是$(R,+)$的子群；

(2) 对任意 $a,b\in S$，有 $a\cdot b\in S$. ▌

命题 3 设$(R,+,\cdot)$是个环，S 是 R 的非空子集. 那么，S 是 R 的子环的充分必要条件是

(1)* 对任意 $a,b\in S$，有 $a-b\in S$；

(2)* 对任意 $a,b\in S$，有 $a\cdot b\in S$. ▌

为了检查自己对子环概念理解的深刻程度，你也可以不去翻群论中的结论而直接按定义证明上述两命题.

例 5 整数环 $\mathbf{I}$ 的子集中，所有偶数的集 E 是 $\mathbf{I}$ 的子环，因为它在减法和乘法之下封闭；所有奇数的集合 Q 不是 $\mathbf{I}$ 的子环，因为 Q 在减法之下不封闭，例如 $7,3\in Q$，但

$$7-3=4\notin Q.$$

也可以说，数的加法不是 Q 上的运算，或说 Q 不是 $\mathbf{I}$ 的加法子群.

例 6 本节例 2 的环$(C,\#,\odot)$中，子集

$$S=\{f\in C\mid f(2)=0\}$$

是 C 的一个子环. 这是因为，对任意 $f,g\in C$，

$$(f-g)(2)=f(2)-g(2)=0,$$

$$(f\odot g)(2)=f(2)g(2)=0,$$

即 $f-g\in S$，$f\odot g\in S$.

命题 4 设 S_α，$\alpha\in I$ 都是环 R 的子环. 那么，它们的交集 $S=\bigcap\limits_{\alpha\in I}S_\alpha$ 必然也是 R 的子环.

分析 不管我们用命题 1 至命题 3 的哪组条件验证，都首先要验证 S 是个非空子集.

作为子集，每个 S_α 都非空并不能保证它们的交集 S 必然非空.

但是，这里的每个 S_α 都是子环，它有更进一步的性质.

证明 学习群论时已经知道，加法群 R 的每个子群 S_α 的零

元素 0_α 必然就是 R 的零元素 0. 由于 $0\in S_\alpha$，$\alpha\in I$，所以

$$0\in \bigcap_{\alpha\in I} S_\alpha = S,$$

从而 S 非空.

进一步，对任意 $a,b\in S$，应有

$$a,b\in S_\alpha, \quad \alpha\in I,$$

而 S_α 是 R 的子环，从而对每个 $\alpha\in I$ 而言，都有 $a-b\in S_\alpha$，再据 S 的定义，必有 $a-b\in S$.

同样，对任意 $a,b\in S$，应有

$$a,b\in S_\alpha, \quad \alpha\in I,$$

而 S_α 是 R 的子环，从而对每个 $\alpha\in I$ 而言，都有 $ab\in S_\alpha$，再据 S 的定义，又有 $ab\in S$.

所以，S 是 R 的子环. ▌

定义 2 设 R 是个环，$a\in R$. 做 R 的子环族

$$A=\{S \text{ 是 } R \text{ 的子环} \mid a\in S\},$$

我们把子环(注意 $R\in A$，A 非空)

$$\bigcap_{S\in A} S$$

称为 R 的**由元素 a 生成的子环**，记为 $\langle a\rangle$.

推论 $\langle a\rangle$ 是 R 的包含 a 的子环中的最小者.

证明 首先，$\langle a\rangle$ 是 R 的一个包含元素 a 的子环.

其次，设 S 是 R 的任意子环，$a\in S$，那么由定义知 $S\in A$，而 $\langle a\rangle$ 是所有 A 中元的交集，当然有 $\langle a\rangle\subseteq S$.

这就意味着 $\langle a\rangle$ 是所有包含 a 的子环中的最小者. ▌

本来也可以直接把推论拿来做 $\langle a\rangle$ 的定义，但需要解释"最小者一定存在"这句话，而现在的定义虽然文字较多，但不需要进一步地解释. 它也便于与前面学过的一个元素生成的子群，后面要学的一个元素生成的理想、子域等相对照.

命题 5' 设 R 是个环，$a\in R$. 那么，R 中所有形如

$$ma, ma+na^2, \cdots,$$

$$m_1a+m_2a^2+\cdots+m_ta^t,\cdots$$

的元素(其中 t 是正整数,m,n,m_i 都是整数)做成的集合 S 恰好就是a 生成的子环$\langle a\rangle$.

证明 取 $t=1$, $m_1=1$,知 $a\in S$.所以 S 是个非空集合.

对任意 $x,y\in S$,按 S 的定义,必有

$$x=m_1a+m_2a^2+\cdots+m_ta^t,\quad y=n_1a+n_2a^2+\cdots+n_ra^r,$$

其中 t 和 r 是正整数,$m_1,\cdots,m_t$ 和 $n_1,\cdots,n_r$ 均为整数.不妨设 $t\geqslant r$,于是可将 y 写成

$$y=n_1a+\cdots+n_ra^r+n_{r+1}a^{r+1}+\cdots+n_ta^t,$$

其中 $n_{r+1}=\cdots=n_t=0$.于是

$$x-y=(m_1-n_1)a+\cdots+(m_t-n_t)a^t,$$

且诸 m_i-n_i 仍为整数,所以 $x-y\in S$.

同时

$$xy=m_1n_1a^2+\cdots+m_tn_ra^{t+r},$$

仍有 $xy\in S$.

所以,S 是R 的一个子环,且 $a\in S$.

S 是含a 的子环,而$\langle a\rangle$是 R 中所有含a 的子环的交集,故当然有$\langle a\rangle\subseteq S$.

另一方面,$\langle a\rangle$是个含 a 的子环,故

$$a,a^2,\cdots,a^t\in\langle a\rangle,\quad t\text{ 为任意正整数},$$

进而对任意整数 $m_1,m_2,\cdots,m_t$ 亦有

$$m_1a,\cdots,m_ta^t\in\langle a\rangle,$$

$$m_1a+m_2a^2+\cdots+m_ta^t\in\langle a\rangle.$$

也就是说,S 中的每个元素都在$\langle a\rangle$中,即 $S\subseteq\langle a\rangle$.

总之,有 $S=\langle a\rangle$. ▌

例如,我们看整数环 **I** 中元素 8 生成的子环$\langle 8\rangle$.它的元素应该形如

$$m8+n64+\cdots+k8^t.$$

但由于 $n\cdot 64=8n\cdot 8$，形如 $n64$ 的元素已经包含在 $m8$ 类型里了．所以，$m8$ 概括了〈8〉元素的全体，故

$$\langle 8\rangle=\{m8\mid m\in \mathbf{I}\}.$$

也就是 $\langle 8\rangle=\{\cdots -8,8,16,\cdots\}$．

又比如，在实数环 $\mathbf{R}$ 中看 $\sqrt[3]{2}$ 生成的子环 $\langle\sqrt[3]{2}\rangle$．它的元素应该形如

$$m_1\sqrt[3]{2}+m_2\sqrt[3]{2^2}+\cdots+m_t\sqrt[3]{2^t},$$

但是

$$m_3\sqrt[3]{2^3}=2m_3,\quad m_4\sqrt[3]{2^4}=2m_4\sqrt[3]{2},$$

于是可以把 m_1 与 $2m_4$ 合并，m_2 与 $2m_5$ 合并，知 $\langle\sqrt[3]{2}\rangle$ 元素的一般形式 $2m+n\sqrt[3]{2}+t\sqrt[3]{2^2}$，$m,n,t\in \mathbf{I}$．

进一步，对于环 R 的任意一个非空子集 T，作 R 的子环族（注意 R 本身是 A 的一个元素）

$$A=\{S\text{ 是 }R\text{ 的子环},T\subseteq S\},$$

又可得到一子环

$$\bigcap_{S\in A}S$$

通常称之为 T 生成的**子环**，记为 $\langle T\rangle$．

命题 6 设 T 是环 R 的非空子集，则 T 在 R 中生成的子环恰为由下述形式元素组成的集合，

$$a_1+\cdots+a_n+b_1c_1+\cdots+b_mc_m+d_1e_1f_1+\cdots+d_te_tf_t+\cdots+x_1x_2\cdots x_l+\cdots+z_1z_2\cdots z_l,\qquad (*)$$

其中诸 $a_i,b_j,\cdots,z_k$ 均为 T 中元素或它们的负元．

证明 由于 $a_i,b_j,\cdots,z_k$ 均为集合 T 的元素或其负元，对于 R 的任意子环 S，如果 $T\subseteq S$，据子环的定义，该（$*$）型元必然在 S 中．从而每个（$*$）型元素在所有包含 T 的子环的交集中，也就是每个（$*$）型元必然在 T 生成的子环中．

另一方面，任意两个（$*$）型元素之和、差仍然是（$*$）型元．又

由环的分配律可算出来，任意两个(＊)型元素之积亦必为(＊)型元. 也就是说，所有(＊)型元素构成 R 的一个子环. 而且此子环包含 T.

设 R 中所有(＊)元素的集合为 T^*. 上述事实说明 $\langle T\rangle\supseteq T^*$，而 T^* 又是含 T 的子环，故 $T^*\supseteq\langle T\rangle$. 所以，$\langle T\rangle=T^*$.

证明中并没要求(＊)元有表法唯一性. 既使 $a_1,\cdots,a_n$ 中有某些是重复的，可写成

$$a_1+a_2+\cdots+a_n=m_1a_{i_1}+\cdots+m_ta_{i_t},$$

即把所有相同的元和它们的负元素合并记在一起，我们也可以不合并. ∎

现在看 $T=\{a,b\}$，即 T 只含 2 个元素的这种比较简单的情形.

此时，(＊)中 $a_1+\cdots+a_n$ 无非就是 T 中 m 个元素与若干个负元素之和. 归并之，即 $ka+lb,\ k,l\in\mathbf{I}$.

同样，$b_1c_1+\cdots+b_mc_m$ 中之 b_i 和 c_j 只能是 $\pm a,\pm b$，归并之，即

$$sa^2+pab+qba+tb^2,\quad s,p,q,t\in\mathbf{I}.$$

对于 3 个元素相乘形式，它们可并成

$$ma^3+na^2b+sab^2+tb^3+iaba+jbab+kba^2+lb^2a,$$

其中 m,n,s,t,i,j,k,l 都是整数.

……

这样，一般项就被合并了.

如果 a 和 b 还可以交换，即 $ab=ba$，那么各项还可以进一步合并.

例题 3 求出整数环 $\mathbf{I}$ 中 6 和 9 生成的子环 $\langle 6,9\rangle$.

解 此子环含所有形如

$$k6+l9,\quad k,l\in\mathbf{I}\qquad (*)$$

形式的整数，而 $\mathbf{I}$ 是交换环

$$s6^2+p(6\cdot 9)+t9^2=(6s+9p)6+(9t)9,$$

也具有(*)形式.同样

$$m6^3+n6^2\cdot 9+\cdots$$

也可写成(*)形式.所以,

$$k6+l9,\quad k,l\in \mathbf{I}$$

就代表了子环$\langle 6,9\rangle$的所有元素.

进一步,由于 $k6+l9=(2k+3l)3\in\langle 3\rangle$,且 $3=(-1)6+9\in\langle 6,9\rangle$,知得$\langle 6,9\rangle=\langle 3\rangle$. ∎

这个例子告诉我们,任意给定的子集 T 所生成的子环的元素表达起来形式比较复杂.但对于具体的环,具体的子集,却有可能进行合并和化简,表达起来很简单.

例题 4 在所有实的 2 阶矩阵构成的环 $M_2(\mathbf{R})$中,求其子集

$$T=\left\{\begin{pmatrix}0 & m\\ n & 0\end{pmatrix}\middle|\, m,n\in \mathbf{I}\right\}$$

生成的子环.

分析 T 中若干个元素之和仍具有

$$\begin{pmatrix}0 & m\\ n & 0\end{pmatrix},\quad m,n\in \mathbf{I} \tag{1}$$

形式.再看任意两个 T 中元之积,由于

$$\begin{pmatrix}0 & m\\ n & 0\end{pmatrix}\begin{pmatrix}0 & l\\ k & 0\end{pmatrix}=\begin{pmatrix}mk & 0\\ 0 & ln\end{pmatrix},$$

可以看出$\langle T\rangle$必然包含所有形如

$$\begin{pmatrix}s & 0\\ 0 & t\end{pmatrix},\quad s,t\in \mathbf{I} \tag{2}$$

的元.由(1)型元与(2)型元做和,即得 $\mathbf{I}$ 上所有 2 阶矩阵.

本来还要继续看 3 个(1)型元素之积,等等,但 $\mathbf{I}$ 上所有 2 阶矩阵构成 $M_2(\mathbf{R})$的子环.由$\langle T\rangle$之最小性,我们就不必再探讨其扩大的可能性了.

解 用 $M_2(\mathbf{I})$代表所有整的 2 阶矩阵所构成的环.显然,

$$T \subseteq M_2(\mathbf{I}).$$

另一方面,对于 $M_2(\mathbf{R})$的包含 T 的任意一个子环 S,由于

$$\begin{pmatrix} 0 & k \\ l & 0 \end{pmatrix} \in S, \quad 对任意\ k, l \in \mathbf{I},$$

故

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & k \\ l & 0 \end{pmatrix} = \begin{pmatrix} l & 0 \\ 0 & k \end{pmatrix} \in S,$$

又因为,对任意 $m, n \in \mathbf{I}$ 恒有

$$\begin{pmatrix} 0 & m \\ n & 0 \end{pmatrix} \in S,$$

所以,对任意 $m, n, k, l \in \mathbf{I}$,均有

$$\begin{pmatrix} l & m \\ n & k \end{pmatrix} \in S$$

也就是 $M_2(\mathbf{I}) \subseteq S$,即 $M_2(\mathbf{I})$是含 T 的最小子环.

从而得到,$M_2(\mathbf{I}) = \langle T \rangle$. ▌

在群的理论中,正规子群(即不变子群)作用巨大,地位重要.

设$(G, \cdot)$是个群,H 是它的正规子群,那么,对任意陪集 aH, bH 可以规定

$$aH \cdot bH = abH \qquad (*)$$

使得等价类的集合 G/H 也构成一个群.

在那里,我们特别强调,只有对正规子群而言,(*)规定的运算才是合理的,也就是此时可保证,如果 $aH = a_1 H$, $bH = b_1 H$,则必有

$$abH = a_1 b_1 H,$$

即(*)的规定与每个陪集的代表元的选取没有关系.否则,(*)的规定不会导出 G/H 上的确定的运算.

现在,我们讨论环$(R, +, \cdot)$.由于$(R, +)$是交换群,它的每个子群都是其正规子群.所以,对于$(R, +)$的任意子群$(A, +)$.

完全抛开乘法不管，只把它们作为群的讨论，则

$$G/A=\{a+A,b+A,\cdots\}$$

是个加法群. 如果 G/A 的加法记为 #，则对任意 $a+A,b+A\in G/A$ 都有 $(a+A)\#(b+A)=(a+b)+A$.

但是，R 是有乘法的，能不能由 R 的乘法自然的引出 R/A 上的一个乘法呢？对任意陪集 $a+A,b+A$，令其对应 $ab+A$，是否就建立了 G/A 上的一个乘法泥？

关键在于，上面所说的“对应”

$$(a+A,b+A)\rightarrow ab+A$$

是否是 $(G/A)\times(G/A)$ 到 G/A 的映射. 必须注意，这里随便说了个“对应”是不对的. 集合间的映射中所用的“对应”概念是有严格的含义的. 具体到这里来，应该要求，对陪集 $a+A,b+A$ 按给定的办法要有唯一确定的陪集与之对应. 必须与陪集代表元选择无关. 不能随便一说了之.

要使“与陪集之代表元选择无关”一事成立，即要求，若 $a+A=a_1+A,b+A=b_1+A$ 必有

$$ab+A=a_1b_1+A.$$

让我们仔细分析一下这个要求. 条件

$$a+A=a_1+A,\quad b+A=b_1+A,$$

即有 $x\in A$, $y\in A$ 使

$$a+x=a_1,\quad b+x=b,$$

于是，

$$a_1b_1=(a+x)(b+y)=ab+ay+xb+xy.$$

想要有 $a_1b_1+A=ab+A$，只要使

$$ay+xb+xy\in A$$

就行了.

如果 A 是 $(R,+\cdot)$ 的子环，由于 $x,y\in A$，就保证了 $xy\in A$. 仍不能保证对任意 $x,y\in A$ 和任意 $a,b\in R$ 都有 $ay+xb\in A$.

于是,需引出下列的

定义 3 设$(R,+,\cdot)$是个环,A 是R 的非空子集.如果

(1) $(A,+)$是$(R,+)$的子群;

(2) 对任意 $x,y\in A$ 和任意$a,b\in R$ 都有$ay\in A$, $xb\in A$,

则说 A 是R 的**理想**.

从定义中可以看出,A 为 R 的理想则 A 必为 R 的子环.因此,有人也称环的理想为环的**理想子环**.

又因为条件(2)体现了两侧要求,即对任意 $x\in A$,从右乘以 R 的任意元b,要求 $xb\in A$;同时,对任意 $y\in A$,从左侧乘以 R 的任意元 a,要求 $ay\in A$.因此,有时称环的理想为其**双侧理想**或**双边理想**.

例 7 所有 2 阶整数方阵作成的环 $M_{2\times 2}$中,所有元素恒为偶数的方阵集 $E_{2\times 2}$是 $M_{2\times 2}$的一个理想.

$E_{2\times 2}$对矩阵减法封闭,它是 $M_{2\times 2}$的一个加法子群.

任取

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in M_{2\times 2},\quad \begin{pmatrix} 2m & 2p \\ 2n & 2q \end{pmatrix}\in E_{2\times 2}$$

都有

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 2m & 2p \\ 2n & 2q \end{pmatrix}=\begin{pmatrix} 2(ma+nb) & 2(pa+qb) \\ 2(mc+nd) & 2(pc+qd) \end{pmatrix}\in E_{2\times 2},$$

另一侧条件的验证道理相同.

例 8 整数环$(\mathbf{I},+,\cdot)$中,对一固定正整数 n,集合

$$A=\{\cdots,-2n,-n,0,n,2n,\cdots\}$$

是 $\mathbf{I}$ 的理想.

A 对减法封闭,A 是 $\mathbf{I}$ 的加法子群.

$\mathbf{I}$ 是交换环,条件(2)之两侧要求变成同一要求.对任意 $x\in A$, $a\in\mathbf{I}$,设 $x=kn$, k 为某个整数.于是

$$a\cdot x=a\cdot kn=(ka)n\in A.$$

A 是 $\mathbf{I}$ 的理想.

例 9 设 P 是所有实系数多项式作成的环，F 是所有常数项恒为 0 实系数多项式的集合. 那么，F 是 P 的理想.

任取 F 中元素 $f(x)$，$g(x)$，它们的常数项为 0，从而 $f(x)-g(x)$ 之常数项亦为 0，也就是说 $f(x)-g(x)\in F$. 所以，F 是 P 的加法子群.

对任意 $f(x)\in F$，$a(x)\in P$，由于 $f(x)$ 之常数项为 0，故 $a(x)f(x)$ 之常数项必为 0，即

$$a(x)f(x)\in F.$$

又因 P 是交换环，验证一侧条件就够了.

F 是 P 的理想.

例 10 在例 7 的 $M_{2\times 2}$ 中，所有形如

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}, \quad b, a \text{ 为整数},$$

的矩阵的集合 A 是 $M_{2\times 2}$ 的子环，但 A 不是 $M_{2\times 2}$ 的理想.

要验证 A 为 $M_{2\times 2}$ 的子环是容易的.

进一步，对任意整数 m, n, p, q，都有

$$\begin{pmatrix} m & p \\ n & q \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}=\begin{pmatrix} ma+pb & 0 \\ na+qb & 0 \end{pmatrix}\in A,$$

即 A 还满足条件(2)的左侧条件.

但是，取

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\in A, \quad \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\in M_{2\times 2},$$

则

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\notin A,$$

这说明 A 不是 $M_{2\times 2}$ 的理想.

与子集生成的子环概念平行地，我们需要研究子集生成的理想的特点.

命题 7 设 R 是个环，A_α，$\alpha\in I$ 都是 R 的理想. 那么，它们

的交集 $A=\bigcap_{\alpha\in I}A_\alpha$ 必然也是 R 的理想.

证明 对于每个 $\alpha\in I$, A_α 都是 R 的理想, A_α 当然是 R 的子环. 利用命题 4 可知,它们的交集 A 必然是 R 的子环.

进一步,对任意 $a\in A$, $r\in R$. 由于 A 是诸 A_α 之交集,故对每个 α 恒有 $a\in A_\alpha$,又由于 A_α 均为 R 之理想,从而对每个 $\alpha\in I$ 都有

$$ra\in A_\alpha,\quad ar\in A_\alpha.$$

进而, ra 和 ar 必在所有 A_α 的交集 A 中,即

$$ra\in A,\quad ar\in A.$$

这说明 A 是 R 的理想. ▌

再提醒读者注意, R 本身是 R 的理想,而且它包含 R 的每个子集. 也可以说, R 的任意子集都包含在某些理想中.

有了这些准备,即可给出

定义 4 设 R 是个环, $T\subseteq R$, T 非空. 作 R 的理想族

$$B=\{I\text{ 是 }R\text{ 的理想}, T\subseteq I\}$$

得到的理想

$$\bigcap_{I\in B}I$$

称之为 R 的**由子集 T 生成的理想**,记为 (T).

特别地,如果 T 仅有一个元素 a,则把理想 $(\{a\})$ 记为 (a),并称为是由 a 生成的**主理想**.

定理 1 设 T 是环 R 的非空子集. 那么, R 中所有形如 $(*)$ 的元素的集合恰为 (T),所谓 $(*)$ 型元者乃有如

$$\begin{aligned}&n_1a_1+\cdots+n_ta_t+r_1b_1+\cdots+r_kb_k\\&+c_1s_1+\cdots+c_ls_l+x_1d_1y_1+\cdots+x_id_iy_i,\end{aligned}\qquad(*)$$

其中 $n_1,\cdots,n_t$ 是整数, $a_1,\cdots,a_t$; $b_1,\cdots,b_k$; $c_1,\cdots,c_l$ 和 $d_1,\cdots,d_i$ 是 T 中元素. 而 $r_1,\cdots,r_k$; $s_1,\cdots,s_l$ 和 $x_1,\cdots,x_i$ 及 $y_1,\cdots,y_i$ 是 R 的元素.

证明 可与 T 生成的子环 $\langle T\rangle$ 构成情形的证明采取完全一

致的步骤(对照命题6).即逐步证实如下论断:

(1) 对 R 的任意理想 $I, T\subseteq I$,则 I 必然包含所有的($*$)型元;

(2) 进而,(T)包含所有($*$)型元素;

(3) 两个($*$)型元之差仍为($*$)元;

(4) 对任意 $r\in R$,只要 $a_1, b_1, c_1, d_1\in T$,则

$$r(n_1a_1)=(n_1r)a_1,\quad r(r_1b_1)=(rr_1)b_1,$$

$$r(c_1s_1)=rc_1s_1,\quad r(x_1d_1y_1)=(rx_1)d_1y_1$$

都是($*$)型元素.利用环的分配律可以说明,r 乘($*$)型元仍得($*$)型元.

(5) 所有($*$)型元的集合是 R 的一个理想.

(6) 该集包含在$\langle T\rangle$中,反过来又要包含$\langle T\rangle$,故二者相等.

▍

推论 1 设 R 是个环,$a\in R$.那么$\langle a\rangle$恰为所有形如下的元素构成的集合:

$$na+ra+as+x_1ay_1+\cdots+x_iay_i,$$

其中 n 为整数,$r, s, x_1, \cdots, x_i$ 和 $y_1, \cdots, y_i$ 都是 R 中元素. ▍

推论 2 设 R 是个有恒等元素 e 的环,$a\in R$.那么 a 生成的主理想(a)恰为所有形如下的元素构成的集合:

$$x_1ay_1+\cdots+x_jay_j, \qquad (*\ *)$$

其中 $x_1, \cdots, x_j$ 和 $y_1, \cdots, y_j$ 是 R 的任意元素.

这是因为,对于环 R,(a)中元

$$na=n(ea)=(ne)a=(ne)ae,$$

$$ra=rae,\quad as=eas,$$

从而每个(a)中元素均可表成($*\ *$)型. ▍

例题 5 在整数环$(R, +, \cdot)$中,每个子环 S 必定是由某个非负整数生成的主理想.

证明 如果 S 只含有 0 元,那么 $S=(0)$.

若有非 0 整数 $m\in S$，则 S 必含有正整数. 看 S 中的最小的正整数 n.

对于 S 中的任意整数 t，用 n 去除 t 得

$$t=qn+r,\quad 0\leqslant r<n.$$

由于 S 是子环，qn 乃是若干个 n 之和或若干个 $-n$ 之和，故 $qn\in S$. 所以

$$t-qn=r\in S.$$

由 n 的最小性，可推出 $r=0$，即 $t=qn$.

所以，$S=\{xn\mid x\in \mathbf{I}\}$ 恰是 n 生成的主理想. ▌

事实上，在第二章 §4，我们早就证明过，整数环$(\mathbf{I},+)$的每个子群必然是由某个非负整数 n 生成的.

现在又证明了一遍，技巧相同，得出，整数环$(\mathbf{I},+,\cdot)$的每个理想也必是由某个非负整数生成的.

$\mathbf{I}$ 的每个加法子群都是作为环时的理想，这类环是很特殊的.

设 A,B 都是环 R 的理想，用$(A\cup B)$代表集合 $A\cup B$ 在 R 中生成的理想，再令

$$A+B=\{x\in R\mid x=a+b,\ a\in A,\ b\in B\}.$$

并称为是理想 A,B 的和. 有

命题 8 设 A,B 是 R 的理想. 那么 $A+B=(A\cup B)$.

证明 首先，可断言 $A+B$ 是 R 的理想.

对任意 $x,y\in A+B$，设

$$x=a+b,\ y=c+d,\quad a,c\in A,\ b,d\in B$$

则必有 $x-y=(a-c)+(b-d)\in A+B$.

对任意 $x=a+b\in A+B$ 及 $r\in R$，恒有

$$rx=r(a+b)=ra+rb\in A+B,$$

同理又有 $xr\in A+B$.

这说明 $A+B$ 是 R 的理想. 任意 $a\in A$ 均可写成 $a=a+0\in A+B$，从而 $A\cup B$ 包含在理想 $A+B$ 之中. 据$(A\cup B)$的定义，得

$$(A\cup B)\subseteq A+B.$$

另一方面，$(A\cup B)$是个理想，且含 A 又含 B，所以，对任意 $a\in A$，$b\in B$，必有

$$a+b\in(A\cup B).$$

从而 $A+B\subseteq(A\cup B)$.

总之，有 $A+B=(A\cup B)$. ▌

例题 6 设 R 是个有单位元的交换环. 给出 $a_1,\cdots,a_n\in R$ 在 R 中生成的理想.

解 看 R 的子集

$$T=\{r_1a_1+\cdots+r_na_n\in R\mid r_1,\cdots,r_n\in R\}.$$

首先，对任意 $s,t\in T$，设

$$s=r_1a_1+\cdots+r_na_n,\quad r_i\in R,$$

$$t=l_1a_1+\cdots+l_na_n,\quad l_j\in R.$$

则

$$s-t=(r_1-l_1)a_1+\cdots+(r_n-l_n)a_n\in T.$$

同时，对任意 $x\in R$，及 $r_1a_1+\cdots+r_na_n\in T$ 有

$$x(r_1a_1+\cdots+r_na_n)=(xr_1)a_1+\cdots+(xr_n)a_n\in T,$$

$$(r_1a_1+\cdots+r_na_n)x=(r_1x)a_1+\cdots+(r_nx)a_n\in T,$$

这说明 T 是 R 的理想.

其次，设 e 是 R 的单位元，则

$$a_i=0a_1+\cdots+ea_i+\cdots+0a_n\in T,$$

又说明 $a_1,\cdots,a_n\in T$.

最后，对 R 的任意理想 A，只要 $a_1,\cdots,a_n\in A$，那么，任取 $r_1,\cdots,r_n\in R$，均有

$$r_1a_1,\cdots,r_na_n\in A,\quad r_1a_1+\cdots+r_na_n\in A.$$

从而 $T\subseteq A$，所以 T 就是 $a_1,\cdots,a_n$ 生成的理想.

此时，我们有

$$T=(a_1,\cdots,a_n)=(a_1)+(a_2)+\cdots+(a_n).$$ ▌

此后，要不断地处理有 1 交换环中各种问题，遇有有限个元素

生成的理想的表达形式时，一般不再解释．特别是一个元素 a 生成的主理想(a)中元素的表达形式读者更应有明确的认识．绝不可以认为，任意环 R 的主理想

$$(a)=\{ra \mid r\in R\}$$

或 $(a)=\{\sum r_i a s_i \mid r_i, s_i \in R\}$.

例题 7 设 A,B 是环R 的非空子集．通常用AB 代表R 中所有形如 $a_1b_1+\cdots+a_nb_n$，$a_i\in A$，$b_j\in B$，n 为正整数，元素构成的集合．证明：当 A,B 都是R 的理想时，集 AB 也是R 的理想．

证明 任取 $x,y\in AB$，设

$$x=a_1b_1+\cdots+a_nb_n,\quad a_i\in A,\ b_j\in B,$$

$$y=c_1d_1+\cdots+c_md_m,\quad c_k\in A,\ d_l\in B,$$

那么

$$x-y=a_1b_1+\cdots+a_nb_n+(-c_1)d_1+\cdots+(-c_m)d_m.$$

由于$-c_1,\cdots,\ c_m$ 亦为A 中元，故 $x-y\in AB$.

再任取 $u\in R$，由于

$$ux=(ua_1)b_1+\cdots+(ua_n)b_n,\quad ua_i\in A,$$

$$xu=a_1(b_1u)+\cdots+a_n(b_nu),\quad b_ju\in B,$$

故 $ux,xu\in AB$.

所以，AB 是环R 的理想． ∎

设 R 是个环，R 的非空子集 S 在其加法之下是R 的加法子群，且对任意 $r\in R$，$x\in S$ 恒有$rx\in S$，则说 S 是R 的一个**左理想**．对称地可引入**右理想**概念．在进一步学习环论和模论时要经常提到它们．但我们这里不做深入探讨．

习 题 二

1. 在环 $\mathbf{I}_6$ 中给出一个子环，它本身是个有恒等元的环，但它的恒等元不是 $\mathbf{I}_6$ 的恒等元 1^*.

2. 设 p 是个素数．证明：有理数环 $\mathbf{Q}$ 的子集

$$H=\left\{\frac{m}{n}\in\mathbf{Q}\mid(m,n)=1\text{ 且}(n,p)=1\right\}$$

构成 $\mathbf{Q}$ 的一个子环.其中 $(k,l)=1$ 表示整数 k 和 l 的最高公因子为1.

3. 设 p 是个素数.证明:有理数环 $\mathbf{Q}$ 的子集

$$K=\left\{\frac{m}{n}\in\mathbf{Q}\mid(m,n)=1\text{ 且 }n=p^k,\ k\geqslant 0\right\}$$

构成 $\mathbf{Q}$ 的一个子环.

4. 给出§1 例5中环 R 的所有子环.

5. 设 R 是个环,那么

$$S=\{x\in R\mid\text{有正整数 }n\text{ 使 }nx=0\}$$

构成 R 的一个理想.

6*. 若 e_1,e_2 是交换环 R 的等方元,即

$$e_1^2=e_1,\quad e_2^2=e_2.$$

证明:R 的由 e_1,e_2 生成的理想 (e_1,e_2) 必定是由某个等方元 f 生成的主理想,即 $(e_1,e_2)=(f)$, $f^2=f$.

§3 理想与商环(Ⅰ)

上一节我们提过,如果 $(R,+,\cdot)$ 是个环,$(S,+,\cdot)$ 是它的子环.由于 $(S,+)$ 是 $(R,+)$ 的加法子群(当然就是正规子群).作为群,可得商群

$$R^*=(R,+)/(S,+).$$

一般来说,不能由此自然地在 R^* 中引入乘法(注意,这里所说自然引入的乘法当然是由 R 的乘法导入的,而不是随便定义一个 R^* 的乘法),使 R^* 成为一个环.

经过分析,如果子环 S 还满足另外的条件,S 是 R 的理想,那么,有可能自然地使 R^* 引入乘法而成为环.现在严格的证明这件事.

定理 1 设 $(R,+,\cdot)$ 是个环,A 是 R 的理想.作为加法群,得商群

$$\overline{R}=R/A,\quad\text{加法}\ \#.$$

在加法群 $\overline{R}$ 中再定义乘法，任意 $a+A, b+A\in\overline{R}$，对应 $ab+A$，记为

$$(a+A)\odot(b+A)=ab+A.$$

则 $(\overline{R},\#,\odot)$ 是个环.

证明 首先要证明乘法 $\odot$ 的定义是合理的，即它与陪集的代表元选择无关. 设

$$a+A=a_1+A,\quad b+A=b_1+A,$$

从而有 $x, y\in A$ 使 $a_1=a+x,\ b_1=b+y$. 于是

$$a_1b_1=(a+x)(b+y)=ab+ay+xb+xy.$$

由于 A 是 R 的理想，$x\in A,\ y\in A$，故

$$ay\in A,\ xb\in A,\ xy\in A,\ ay+xb+xy\in A,$$

即 $a_1b_1-ab\in A$，

$$a_1b_1+A=ab+A.$$

这说明 $\odot$ 确实是 $\overline{R}$ 上的二元运算.

其次要证明 $\overline{R}$ 对 $\odot$ 满足结合律. 任取 $\overline{R}$ 中 3 个元素，也就是 R 对 A 的 3 个陪集. 由于 $\odot$ 运算与陪集之代表元选取无关，在每个陪集中随便取一元做代表，即设 $\overline{R}$ 的 3 个任意元为

$$a+A, b+A, c+A,$$

于是有

$$\begin{aligned}
&[(a+A)\odot(b+A)]\odot(c+A)\\
&\quad=[ab+A]\odot(c+A) && (\odot\text{的定义})\\
&\quad=(ab)c+A && (\odot\text{的定义})\\
&\quad=a(bc)+A && (R\text{ 中乘法结合律})\\
&\quad=(a+A)\odot(bc+A) && (\odot\text{的定义})\\
&\quad=(a+A)\odot[(b+A)\odot(c+A)]. && (\odot\text{的定义})
\end{aligned}$$

最后来验证 $\overline{R}$ 对 $\odot$ 和 $\#$ 有分配律. 任取 $a+A, b+A, c+A\in\overline{R}$. 则

$$(a+A)\odot[(b+A)\#(c+A)]$$

$$=(a+A)\odot((b+c)+A) \qquad (\overline{R}\text{ 中}\#\text{的定义})$$
$$=a(b+c)+A \qquad (\overline{R}\text{ 中}\odot\text{的定义})$$
$$=(ab+ac)+A \qquad (R\text{ 中有分配律})$$
$$=(ab+A)\#(ac+A) \qquad (\overline{R}\text{ 中}\#\text{的定义})$$
$$=((a+A)\odot(b+A))\#((a+A)\odot(c+A)).$$
$$(\overline{R}\text{ 中}\odot\text{的定义})$$

另一侧分配律的验证是类似的.

总之,$(\overline{R},\#)$是交换群,$\overline{R}$ 乘法$\odot$满足结合律,$\odot$和$\#$满足分配律.所以,$(\overline{R},\#,\odot)$是个环. ▌

定义 设 R 是个环,A 是 R 的理想.有商群 $\overline{R}=R/A$ 中规定

$$(a+A)\odot(b+A)=ab+A,\quad a+A,b+A\in\overline{R}$$

得到的环$(\overline{R},\#,\odot)$称为是环$(R,+,\cdot)$对理想 A 的**商环**,或称**剩余环**.

例 1 讨论整数环$(\mathbf{I},+,\cdot)$的所有商环.

任取 $\mathbf{I}$ 的一个理想 A.

如果 $A=\mathbf{I}$,那么 $\mathbf{I}$ 对 A 只有一个陪集,即 A,也就是 $\mathbf{I}/A$ 只有一个元素,可以用数 0 作代表元,

$$(0+A)\#(0+A)=0+A,\quad (0+A)\odot(0+A)=0+A.$$

如果 A 仅含一个元素,$A=\{0\}$.那么每个整数 $m\in\mathbf{I}$ 都单独组成 $\mathbf{I}$ 对$\{0\}$的一个陪集$\{m\}$.在商环 $\mathbf{I}/\{0\}$中,$\{m\}=m+\{0\}$,且

$$(m+\{0\})\#(n+\{0\})=(m+n)+\{0\},$$
$$(m+\{0\})\odot(n+\{0\})=mn+\{0\}.$$

一般情形,若 $A=(n)$, $n\neq0$, $n\neq1$.让我们回顾一下在第二章§4 和第一章§3 已经讨论过的事实.

首先,得 $\mathbf{I}$ 对 A 的商集,

$$\overline{\mathbf{I}}=\mathbf{I}_{\sim n}=\{[0],[1],\cdots,[n-1]\},$$

其中

$$[0]=A=\{\cdots,-n,0,n,\cdots\},$$
$$[1]=1+A=\{\cdots-n+1,0,n+1,\cdots\},$$

$$\cdots,$$

$$[n-1]=(n-1)+A=\{\cdots,-1,n-1,\cdots\}.$$

其次,自然地得到 $\bar{\mathrm{I}}$ 上的加法作成商群

$$[a]+[b]=[a+b],$$

也就是 $(a+A)+(b+A)=(a+b)+A$.

最后,现在又自然地定义 $\bar{\mathrm{I}}$ 上乘法成商环

$$(a+A)(b+A)=ab+A,$$

也就是 $[a][b]=[ab]$.

特别地,取 $n=5$. 看商环 $\bar{\mathrm{I}}=\mathrm{I}/(5)$. 记

$$\bar{\mathrm{I}}=\{[0],[1],[2],[3],[4]\},$$

它自然地有两个二元运算,运算表是

加	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

乘	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

例 2 所有形如

$$\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}, \quad a,b,c \text{ 实数}$$

的 2 阶方阵的集合是实的 2×2 全阵环的一个子环,记为 R. R 中所有形如

$$\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}, \quad x \text{ 是实数},$$

的矩阵的集合 A 是 R 的理想.

这是因为,A 对矩阵减法封闭. A 是 R 的加法子群. 对任意

$$\begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \in R, \quad \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} \in A,$$

有

$$\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ax \\ 0 & 0 \end{pmatrix} \in A,$$

$$\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & c \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & xb \\ 0 & 0 \end{pmatrix} \in A.$$

因为 R 的任意元

$$\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}$$

恒可表成

$$\begin{pmatrix} a & c \\ 0 & b \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} + \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} \in A,$$

故

$$\begin{pmatrix} a & c \\ 0 & b \end{pmatrix} + A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} + A,$$

即 R/A 的每个陪集均可由一对角矩阵作代表元素. R/A 的运算是

$$\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} + A\right) \# \left(\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} + A\right) = \begin{pmatrix} a+c & 0 \\ 0 & b+d \end{pmatrix} + A,$$

$$\left(a\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} + A\right) \odot \left(\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} + A\right) = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix} + A.$$

例 3 如同上节之例 9 一样,用 P 代表所有实系数多项式在通常加法和乘法之下构成的环. 令

$$A = \{f(x) \in P \mid f(a) = 0, \ a \text{ 为固定实数}\}.$$

也就是说,A 是P 中所有以实数a 为其一根的多项式的集合.

若 $f(x),g(x)\in P$,则 $f(a)-g(a)=0$, $f(x)-g(x)\in A$.

若 $f(x)\in A$, $h(x)\in A$,则 $f(a)h(a)=0$.故

$$f(x)h(x)=h(x)g(x)\in A,$$

A 为P 的理想.

我们知道,多项式 $k(x)$以 a 为其一根之充分必要条件是 $x-a$整除$k(x)$,即有 $q(x)\in P$ 使

$$k(x)=(x-a)q(x).$$

所以,$A=\{k(x)\in P\mid k(x)=(x-a)q(x)$,对某 $q(x)\in P\}$.

任取 $h(x)\in P$,看陪集 $h(x)+A$.用 $x-a$ 除多项式$h(x)$得

$$h(x)=q(x)(x-a)+c,$$

其中 c 是个实数.由于 $q(x)(x-a)\in A$,故

$$h(x)+A=c+A,$$

即 P 对A 的陪集恒可由一常数多项式作代表元素.任取 P/A 的两个元素

$$c+A,\quad d+A$$

在 P/A 中的运算是

$$(c+A)\#(d+A)=c+d+A,$$

$$(c+A)\odot(d+A)=cd+A.$$

商环这一概念是环论的核心概念,读者一定要从集合、等价关系、商集、商群逐步过渡,正确理解商环中元素的形式、运算的由来.

例题1 设 R 是个环,子集

$$S=\{a\in R\mid a=xy-yx,\ x,y\in R\}.$$

令 $A=(S)$.证明:R/A 是个交换环.

证明 因为$0=0\cdot0-0\cdot0\in S$, S 非空,(S)有意义.

任取 R/A 中元素,即 R 对A 的陪集$u+A$, $v+A$ 必有

$(u+A)(v+A)-(v+A)(u+A)$

$$
\begin{aligned}
&= (uv + A) - (vu + A) && (R/A \text{ 中乘法定义}) \\
&= (uv - vu) + A && (R/A \text{ 中加减法定义}) \\
&= 0 + A && (uv - vu \in S \subseteq A)
\end{aligned}
$$

而 $A = 0 + A$ 乃是环 R/A 的零元素，故有

$$(u + A)(v + A) = (v + A)(u + A),$$

这说明 R/A 是个交换环 ▌

对任意环 R 而言，R 本身和 $\{0\}$ 都是 R 的理想，通常称它们为 R 的**平凡理想**.

如果环 R 只有两个理想 R 和 $\{0\}$，那么 R 的商环极为明了，这种环称为**单环**或**单纯环**. 比如例 1 中环

$$\bar{\text{I}} = \{[0],[1],[2],[3],[4]\}$$

元数为 5，它的加法子群只有 $\bar{\text{I}}$ 和 $\{[0]\}$，它的理想也只有其本身和 $\{[0]\}$

例题 2* 所有实的 n 阶方阵在矩阵加法和乘法之下构成的环 $M_{n\times n}$ 是个单环.

证明 我们假设 $M_{n\times n}$ 有个理想 A 不等于理想 $\{O_{n\times n}\}$（$O_{n\times n}$ 为 n 阶零矩阵），来证明 A 必然就是理想 $M_{n\times n}$ 本身.

$A \neq \{O_{n\times n}\}$，即 A 除零矩阵 $O_{n\times n}$ 还要包含另外的矩阵 $D \in A$，

$$D = \sum_{i,j=1}^{n} a_{ij} E_{ij} \neq O_{n\times n}.$$

其中 E_{ij} 是第 i 行第 j 列之元素为 1，其余元素均为 0 的那个矩阵

$$E_{11} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \quad E_{12} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix},$$

$\cdots$.

既然矩阵 $D \neq 0$，它至少要有某一个元素不等于 0，设

$$a_{kl} \neq 0, \quad 1 \leqslant k \leqslant n, \quad 1 \leqslant l \leqslant n.$$

我们利用 A 的减法封闭性和乘积的特殊性来证明 A 必含所有矩阵.

注意到乘积

$$E_{ij}E_{pq}$$

只有当 $j\neq p$ 时才不为 0,等于 E_{iq},而 $j\neq p$ 时,该积恒为零矩阵.

由于 $D\in A$, A 为理想,故

$$E_{kk}DE_{ll}=a_{kl}E_{kl}\in A.$$

再由 $a_{kl}\neq 0$,设 E 为恒等矩阵,用 $a_{kl}^{-1}E$ 左乘上面矩阵,仍应有

$$a_{kl}^{-1}E_{a_{kl}}E_{kl}=E_{kl}\in A.$$

进一步,对任意矩阵 E_{st},由于

$$E_{st}=E_{sk}E_{kl}E_{lt},$$

且 $E_{kl}\in A$,故 $E_{st}\in A$.

最后,对 $M_{n\times n}$ 中任意矩阵

$$B=\sum_{i,j}b_{ij}E_{ij},$$

因为 $E_{ij}\in A$, $b_{ij}E_{ij}=(b_{ij}E)E_{ij}\in A$,对所有 i,j 都对,故它们的和 B 也在 A 中. ▌

例题 3 设 $(R,+,\cdot)$ 是个环,~是 R 上的一个等价关系,且

(1) 如果 $a\sim b$,那么,对任意 $c\in R$,均有 $a+c\sim b+c$,

(2) 如果 $a\sim b$,那么,对任意 $c\in R$,均有 $ac\sim bc$, $ca\sim cb$.

则,元素 0 所在的等价类 $K=\{x\in R\mid x\sim 0\}$ 是 R 的一个理想.

证明 任取 $a,b\in K$,即

$$a\sim 0,\quad b\sim 0,$$

将左式两端同加 $(-b)$ 得

$$a-b=a+(-b)\sim 0+(-b)=-b.$$

将右式两端同加 $(-b)$ 又得

$$0=b+(-b)\sim 0+(-b)=-b.$$

由传递性知 $a-b\sim 0$, $a-b\in K$.

任取 $a\in K$ 及 $r\in R$,由于 $a\sim 0$,有

$$ra \sim r0 = 0, \quad ar \sim 0,$$

也就是 $ra, ar \in K$.

K 为 R 的理想. ▌

关于一个理想和它导出的商环之间的关系,在第五章还要深入讨论,本节主要是让读者搞清楚商环的定义和元素形式.

例题 4 用 $M_2(\mathbf{I})$代表所有元素都是整数的 2 阶方阵作成的环.用 $M_2(E)$代表所有元素都是偶数的 2 阶方阵作成的环.先证明 $M_2(E)$是 $M_2(\mathbf{I})$的理想,再给出商环 $M_2(\mathbf{I})/M_2(E)$的结构.

证明 $M_2(E)$是 $M_2(\mathbf{I})$的理想一事读者可以作为简单练习自证.

任取一个整数矩阵 $A \in M_2(\mathbf{I})$,

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a, b, c, d \in \mathbf{I},$$

a 或为奇数或为偶数,b 或为奇数或为偶数……有 16 种不同的可能.

$$A = \begin{pmatrix} 奇 & 偶 \\ 偶 & 偶 \end{pmatrix}, \quad A = \begin{pmatrix} 偶 & 偶 \\ 偶 & 偶 \end{pmatrix}, \quad \cdots.$$

令

$$D_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, D_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, D_2 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, D_3 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

$$D_4 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, D_5 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, D_6 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, D_7 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$D_8 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, D_9 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, D_{10} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, D_{11} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},$$

$$D_{12} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, D_{13} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, D_{14} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, D_{15} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

我们用 $\overline{D_i}$ 代表商环$M_2(\mathbf{I})/M_2(E)$中的元素

$$D_i + M_2(E).$$

因为每个整数 a 总可写出 $2n+0$ 或 $2n+1$，因此，任意 $A\in M_2(\mathbf{I})$ 总可写成

$$A=B+D_i,\quad 某个\ D_i,$$

而 $B\in M_2(E)$. 也就是 $A+M_2(E)=D_i+M_2(E)$.

这说明，商环 $M_2(\mathbf{I})/M_2(E)$ 上共有 16 个元素，由 $D_0,\cdots,D_{15}$ 可完全代表之. 其加法运算表是(结果中将 $\overline{D}$ 都省掉，再由加法交换性，我们只将表填上半部).

加	$\overline{D}_0$	$\overline{D}_1$	$\overline{D}_2$	$\overline{D}_3$	$\overline{D}_4$	$\overline{D}_5$	$\overline{D}_6$	$\overline{D}_7$	$\overline{D}_8$	$\overline{D}_9$	$\overline{D}_{10}$	$\overline{D}_{11}$	$\overline{D}_{12}$	$\overline{D}_{13}$	$\overline{D}_{14}$	$\overline{D}_{15}$
$\overline{D}_0$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\overline{D}_1$	1	0	3													
$\overline{D}_2$	2	3	0													
$\overline{D}_3$	3	2	1	0												
$\overline{D}_4$	4	5	11	10	0											
$\overline{D}_5$	5	4	10	11	1	0										
$\overline{D}_6$	6	7	14	8	9	13	0									
$\overline{D}_7$	7	6	8	14	13	9	1	0								
$\overline{D}_8$	8	14	7	6	12	15	3	2	0							
$\overline{D}_9$	9	13	15	12	6	7	4	5	10	0						
$\overline{D}_{10}$	10	11	5	4	3	2	12	15	9	8	0					
$\overline{D}_{11}$	11	10	4	5	2	3	15	12	13	14	1	0				
$\overline{D}_{12}$	12	15	13	9	8	14	10	11	4	3	6	7	0			
$\overline{D}_{13}$	13	9	12	15	7	6	5	4	11	1	14	8	2	0		
$\overline{D}_{14}$	14	8	6	7	15	12	2	3	1	11	13	9	5	10	0	
$\overline{D}_{15}$	15	12	9	13	14	8	11	7	5	2	7	6	1	3	4	0

商环 $M_2(\mathbf{I})/M_2(E)$ 的乘法表的计算工作量略大些，只要记住，矩阵某元素为 2 时，可将 2 换成 0，等价关系不变. 我们只计算

几项，如

$$\overline{D}_5\cdot\overline{D}_{10}=\begin{pmatrix}1&0\\1&0\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}+M_2(E)=\begin{pmatrix}0&1\\0&1\end{pmatrix}+M_2(E),$$

也就是 $\overline{D}_5\cdot\overline{D}_{10}=\overline{D}_8$.

又如

$$\overline{D}_{12}\cdot\overline{D}_{13}=\begin{pmatrix}0&1\\1&1\end{pmatrix}\begin{pmatrix}1&0\\1&1\end{pmatrix}+M_2(E)=\begin{pmatrix}1&1\\2&1\end{pmatrix}+M_2(E).$$

而

$$\begin{pmatrix}1&1\\2&1\end{pmatrix}-\begin{pmatrix}1&1\\0&1\end{pmatrix}=\begin{pmatrix}0&0\\2&0\end{pmatrix}\in M_2(E).$$

故 $\overline{D}_{12}\cdot\overline{D}_{13}=\overline{D}_{14}$. ▌

读者可以自己再计算几项.

习 题 三

1. 整数环 $\mathbf{I}$ 对于它的理想(9)所作的商环

$$\bar{\mathbf{I}}=\{[0],[1],[2],[3],[4],[5],[6],[7],[8]\}$$

中，哪些元是单位，哪些元是零因子，哪些元的(加法)周期是 3，哪些元的加法周期是 9?

2. 在整数环 $\mathbf{I}$ 对它的理想(16)所作的商环 $\mathbf{I}/(16)$ 中，含有 $\mathbf{I}/(16)$ 的单位的子环只有 $\mathbf{I}/(16)$ 本身.

3. 设 e 是环 R 的恒等元，I 是 R 的理想，证明：$e+I$ 是商环 R/I 的恒等元. 进一步问，若 I 是 R 的理想，R/I 有恒等元，那么 R 一定有恒等元吗?

4. 设 I 是环 R 的理想，$I\neq R$. 如果 R 为无零因子环，那么 R/I 一定为无零因子环吗? 如果商环 R/I 为无零因子环，环 R 就一定为无零因子环吗?

5. 设 I 是环 R 的理想. 若 I 的每个元素的加法周期都有限(即对每个 $x\in I$ 必有一个正整数 n 使得 $nx=0$)，且商环 R/I 的每个元素的加法周期也都有限. 证明：环 R 的每个元素的加法周期都有限.

6*. (在阅读例题 2 中因符号繁杂而感到困难的读者可做如下题目)证明：所有实的 2 阶矩阵构成的环 $M_{2\times 2}$ 是个单环.

§4 环的同态映射

设$(R,+,\cdot)$是个环,$(S,\#,\odot)$也是个环,我们知道,作为加法群,如果有R到S的映射φ,对任意$a,b\in R$都有

$$\varphi(a+b)=\varphi(a)\#\varphi(b),$$

则φ相当本质地反映了R的加法和S的加法结构上的相似性(特别是φ为满射时,这个φ就是一个$(R,+)$到$(S,\#)$的群同态映射).在第三章已做了比较充分的讨论.

现在,R和S除了分别都有加法运算$+$与$\#$外,它们还都有乘法运算$\cdot$与$\odot$.作为环,希望能够建立R到S的这样的映射,它不仅保证了加法结构上的相似性,也要保证有乘法结构上的相似性.

这就提出了建立环的同态映射的要求.

定义1 设$(R,+,\cdot)$和$(S,\#,\odot)$都是环.R到S的映射φ称之为R到S的**环同态映射**,如果对任意$a,b\in R$恒有

$$\varphi(a+b)=\varphi(a)\#\varphi(b),\quad \varphi(a\cdot b)=\varphi(a)\odot\varphi(b).$$

特别地,当φ是满射时,称S是R的同态像.当φ是满射又是单射时,说φ是R到S的**环同构映射**.

如果能在环R和环S间建立一个环同构映射,则说R和S是同构的,记为$R\cong S$.

例1 如同上节例3,用P代表所有实系数多项式在通常多项式加法和乘法之下构成的环,$\mathbf{R}$是实数环.取一固定实数a,建立P到$\mathbf{R}$的映射φ,令每个多项式$f(x)$对应实数$f(a)$,即

$$\varphi: f(x)\to f(a).$$

由于,对任意$f(x),g(x)\in P$恒有

$$\begin{aligned}&\varphi(f(x)g(x))\\ &\quad=f(a)g(a) && (\varphi\text{ 的定义})\\ &\quad=\varphi(f(x))\varphi(g(a)), && (\varphi\text{ 的定义})\end{aligned}$$

且，同时有

$$\begin{aligned}
&\varphi(f(x)+g(x)) \\
&\quad = f(a)+g(a) && (\varphi \text{ 的定义}) \\
&\quad = \varphi(f(x))+\varphi(g(x)), && (\varphi \text{ 的定义})
\end{aligned}$$

故，φ 是 P 到 $\mathbf{R}$ 的一个环同态映射.

还可以证明 φ 是满的.对 $\mathbf{R}$ 中任意实数 b，看多项式

$$f(x)=x+(b-a),$$

即知

$$f(a)=a+b-a=b;$$

从而 $\varphi(f(x))=b$. 即 $\mathbf{R}$ 中任意数都是某个 P 中多项式在 φ 之下的像.

例 2 在第一节之例 3 中，取 $n=3$. 即

$$\mathbf{I}_n=\{0^*,1^*,2^*\},$$

为区别起见，把 $\mathbf{I}_n$ 的运算暂记为 # 和 $\odot$.

#	0^*	1^*	2^*
0^*	0^*	1^*	2^*
1^*	1^*	2^*	0^*
2^*	2^*	0^*	1^*

$\odot$	0^*	1^*	2^*
0^*	0^*	0^*	0^*
1^*	0^*	1^*	2^*
2^*	0^*	2^*	1^*

具体运算是

$$i^* \# j^*=k^*, \quad i+j=3x+k, \quad 0\leqslant k<3,$$
$$i^*\odot j^*=l^*, \quad i\times j=3y+l, \quad 0\leqslant l<3.$$

现在，建立整数环 $\mathbf{I}$ 到 $\mathbf{I}_3$ 的映射 φ，对任意 $m\in\mathbf{I}$，用 3 除 m 得

$$m=3q+r, \quad 0\leqslant r<3,$$

这个 r 是由 m 唯一确定的，令 $\varphi(m)=r^*$，即 $\varphi: m\to r$.

任取 $m,n\in\mathbf{I}$，设

$$\begin{aligned}
m&=3q+r, \quad 0\leqslant r<3, \\
n&=3p+s, \quad 0\leqslant s<3,
\end{aligned} \tag{1}$$

$$r+s=3x+u,\quad 0\leqslant u<3.$$

则有

$$m+n=3(p+q+x)+u,\quad 0\leqslant u<3.$$

故 $\varphi(m+n)=u^*$.

另一方面,

$$\begin{aligned}\varphi(m)\#\varphi(n)&=r^*\#s^* &&(\varphi\text{ 的定义})\\&=u^*. &&(\text{运算}\#\text{的定义})\end{aligned}$$

所以,$\varphi(m)\#\varphi(n)=\varphi(m+n)$.

这段验证方法读者应该是熟悉的,因为在讲群的同态理论中涉及过.

再来验证 φ 与乘法的关系.接续(1)式,再设

$$r\times s=3y+v,\quad 0\leqslant v<3,$$

就有

$$m\times n=3(q\times s+p\times r)+3p\times q+3y+v,$$

且 $0\leqslant v<3$,故 $\varphi(m\times n)=v^*$.

而且

$$\begin{aligned}\varphi(m)\odot\varphi(n)&=r^*\odot s^* &&(\varphi\text{ 的定义})\\&=v^*, &&(\text{运算}\odot\text{的定义})\end{aligned}$$

所以,$\varphi(m\times n)=\varphi(m)\odot\varphi(n)$.

例 3 研究§3之例2.环 R 是所有形如

$$\begin{pmatrix}a & c\\0 & b\end{pmatrix},\quad a,b,c\text{ 是实数},$$

的矩阵构成的环.令

$$\varphi:\begin{pmatrix}a & c\\0 & b\end{pmatrix}\to\begin{pmatrix}a & 0\\0 & b\end{pmatrix},$$

这是 R 到 R 的映射.且对 R 中任意两个矩阵

$$\begin{pmatrix}a & c\\0 & b\end{pmatrix},\begin{pmatrix}u & w\\0 & v\end{pmatrix},$$

恒有

$$\varphi\left(\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}\begin{pmatrix} u & w \\ 0 & v \end{pmatrix}\right),$$

$$= \varphi\left(\begin{pmatrix} au & aw+cv \\ 0 & bv \end{pmatrix}\right) \qquad \text{(矩阵乘法定义)}$$

$$= \begin{pmatrix} au & 0 \\ 0 & bv \end{pmatrix} \qquad (\varphi \text{ 的定义})$$

$$= \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix} \qquad \text{(矩阵乘法定义)}$$

$$= \varphi\left(\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}\right)\varphi\left(\begin{pmatrix} u & w \\ 0 & v \end{pmatrix}\right), \qquad (\varphi \text{ 的定义})$$

同时

$$\varphi\left(\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}\right) + \begin{pmatrix} u & w \\ 0 & v \end{pmatrix}$$

$$= \varphi\left(\begin{pmatrix} a+u & c+w \\ 0 & b+v \end{pmatrix}\right) \qquad \text{(矩阵加法之定义)}$$

$$= \begin{pmatrix} a+u & 0 \\ 0 & b+v \end{pmatrix} \qquad (\varphi \text{ 的定义})$$

$$= \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} + \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix} \qquad \text{(矩阵加法之定义)}$$

$$= \varphi\left(\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}\right) + \varphi\left(\begin{pmatrix} u & w \\ 0 & v \end{pmatrix}\right). \qquad (\varphi \text{ 的定义})$$

所以，φ 是 R 到自己的一个同态映射，它不是满射，因为 R 中任何矩阵在 φ 之下均不对应矩阵

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

而且，φ 也不是单射，因为

$$\varphi\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\right) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

例 4 研究环 $\mathbf{I}_4$ 和 $\mathbf{I}_2$. 为区别起见把 $\mathbf{I}_2$ 中元素上的 * 号换成

号，即

$$\mathbf{I}_4=\{0^*,1^*,2^*,3^*\},\quad \mathbf{I}_2=\{0^\circ,1^\circ\}.$$

令

$$\varphi(0^*)=\varphi(2^*)=0^\circ,\quad \varphi(1^*)=\varphi(3^*)=1^\circ.$$

也就是说，对任意 $i^*\in\mathbf{I}_4$，i 为偶数时，$\varphi(i^*)=0^\circ$；i 为奇数时，

$$\varphi(i^*)=1^\circ.$$

现断言 φ 是个同态映射.

对任意 $i^*,j^*\in\mathbf{I}_4$，设 $i^*+j^*=r^*$，即

$$i+j=4q+r,\quad 0\leqslant r<4. \tag{2}$$

如果 i 和 j 的奇偶性相同，则 r 为偶数. 故

$\varphi(i^*+j^*)$

$=\varphi(r^*)$ （$\mathbf{I}_4$ 中加法定义）

$=0^\circ$ （φ 的定义，r 为偶数）

$=\varphi(i^*)+\varphi(j^*)$. （两项同时为 0° 或同为 1°）

如果 i 和 j 奇偶性不同，(2)中 r 必为奇数. 故

$\varphi(i^*+j^*)$

$=\varphi(r^*)$ （$\mathbf{I}_4$ 中加法定义）

$=1^\circ$ （φ 的定义）

$=\varphi(i^*)+\varphi(j^*)$. （两项一为 0°，一为 1°）

同样，再设 $i^*\times j^*=t^*$，即

$$i\times j=4p+t,\quad 0\leqslant t<4 \tag{3}$$

若 i 和 j 至少有一个为偶数，不妨假定 i 为偶数，于是 t 为偶数，且

$\varphi(i^*\times j^*)$

$=\varphi(t^*)$ （$\mathbf{I}_4$ 中乘法的定义）

$=0^\circ$ （φ 的定义，t 为偶数）

$=0^\circ\times\varphi(j^*)$ （0°是零元素）

$=\varphi(i^*)\times\varphi(j^*)$. （$\varphi$ 的定义，i 为偶数）

若 i 和 j 都是奇数，则(3)中 t 亦为奇数，故

$$
\begin{aligned}
&\varphi(i^* \times j^*)\\
&\quad = \varphi(t^*) && (\mathbf{I}_4 \text{ 中的乘法的定义})\\
&\quad = 1^\circ && (\varphi \text{ 的定义}, t \text{ 为奇数})\\
&\quad = \varphi(i^*) \times \varphi(j^*). && (\varphi(i^*) = \varphi(j^*) = 1^\circ)
\end{aligned}
$$

所以，φ 是 $\mathbf{I}_4$ 到 $\mathbf{I}_2$ 的满的同态.

设 φ 是环$(R,+,\cdot)$到环$(S,\#,\odot)$的环同态映射. φ 首先是交换群$(R,+)$到交换群$(S,\#)$的群同态映射. 我们可以把第三章中得到的关于群的同态的各种结论全部搬到这里来. 例如

(1) 设 0_1 是 R 的零元素，0_2 是 S 的零元素，则 $\varphi(0_1) = 0_2$；

(2) 用 $-_1$ 代表 R 的减法，$-_2$ 代表 S 的减法，则对任意 a，$b \in R$ 恒有 $\varphi(a -_1 b) = \varphi(a) -_2 \varphi(b)$.

(3) 对任意整数 m，有

$$\varphi(ma) = m\varphi(a), \quad a \in R.$$

又比如，环同态映射 φ 是单射的充分必要条件是它作为群同态映射时为单射；而群同态映射为单射的充要条件是它只把零元素变成零元素. 所以，我们讨论环同态时要不断地利用群论中的成果，同时还要注意乘法条件的作用.

先给出两个重要概念.

定义 2 设 φ 是环$(R,+,\cdot)$到环$(S,\#,\odot)$的环同态映射，那么，称集合

$$\operatorname{Img}(\varphi) = \{s \in S \mid \text{有 } r \in R \text{ 使 } s = \varphi(r)\}$$

为映射 φ 的像，称集合

$$\operatorname{Ker}(\varphi) = \{r \in R \mid \varphi(r) = 0\}$$

为映射 φ 的核.

命题 1 设 φ 是环$(R,+,\cdot)$到环$(S,\#,\odot)$的环同态映射. 那么 φ 的像 $\operatorname{Img}(\varphi)$是环 S 的子环.

证明 对任意 $x, y \in \operatorname{Img}(\varphi)$，设

$$x=\varphi(a), y=\varphi(b), \quad a,b\in R.$$

于是

$$x-y=\varphi(a)-\varphi(b)=\varphi(a-b)\in \mathrm{Img}(\varphi),$$
$$x\odot y=\varphi(a)\odot\varphi(b)=\varphi(a\cdot b)\in \mathrm{Img}(\varphi),$$

即 $\mathrm{Img}(\varphi)$对减法和乘法均封闭.故 $\mathrm{Img}(\varphi)$是环 S 的子环. ▌

一般地,$\mathrm{Img}(\varphi)$未必是环 S 的理想.例 3 中的同态映射 φ 的像即所有实对角形 2 阶矩阵的集合,它不是 R 的理想.因为,有

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}=\varphi(\begin{pmatrix}1&0\\0&1\end{pmatrix})\in \mathrm{Img}(\varphi),$$

但有

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}=\begin{pmatrix}1&1\\0&1\end{pmatrix}\notin \mathrm{Img}(\varphi).$$

命题 2 设 φ 是环$(R,+,\cdot)$到环$(S,\#,\odot)$的同态映射.如果 φ 是满的,R 有恒等元 e,则环 S 必有恒等元,而且恰好就是 $\varphi(e)$.

证明 在第一章就证明过,集合上一个二元运算满足结合律,如果有恒等元,则必唯一.对任意 $x\in S$,由于 φ 是满射,必有 $a\in R$使得 $\varphi(a)=x$.故

$$\begin{aligned}
&\varphi(e)\odot x\\
&\quad=\varphi(e)\odot\varphi(a) && (\varphi\text{ 是满射},x=\varphi(a))\\
&\quad=\varphi(e\cdot a) && (\text{同态性质})\\
&\quad=\varphi(a) && (e\text{ 是}R\text{ 的恒等元})\\
&\quad=x. && (x=\varphi(a))
\end{aligned}$$

同理,$x\odot\varphi(e)=x$.所以 $\varphi(e)$就是 S 的恒等元素. ▌

一般地,e 是R 的恒等元,φ 不是满射,则 $\varphi(e)$未必是 S 的恒等元.例如,R_1 是所有实的对角 2 阶矩阵构成的环,S_1 是所有形如

$$\begin{pmatrix}a&0\\0&0\end{pmatrix},\quad a\text{ 为实数}$$

构成的环,映射

$$\varphi:\begin{pmatrix}a & 0\\0 & b\end{pmatrix}\to\begin{pmatrix}a & 0\\0 & 0\end{pmatrix}$$

显然是 R_1 到 S_1 的环同态.元素

$$\varphi(\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix})=\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$$

恰为 S_1 的恒等元.

但是,我们也可以说 φ 是 R_1 到 R_1 的环同态映射,而元素

$$\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$$

却不是 R_1 的恒等元素.

命题 3 设 φ 是环 $(R,+,\cdot)$ 到环 $(S,\#,\odot)$ 的满的同态映射.那么,如果 R 是交换的,则 S 必然也是交换的.

证明 任取 $x,y\in S$,由于 φ 是满射,故必有 $a,b\in R$ 使得 $x=\varphi(a)$, $y=\varphi(b)$.于是

$$\begin{aligned}
&x\odot y\\
&=\varphi(a)\odot\varphi(b) && (\varphi\text{ 是满的})\\
&=\varphi(a\cdot b) && (\varphi\text{ 是同态映射})\\
&=\varphi(b\cdot a) && (R\text{ 是交换环})\\
&=\varphi(b)\odot\varphi(a) && (\varphi\text{ 是同态映射})\\
&=y\odot x. && (y=\varphi(b),\ x=\varphi(a))
\end{aligned}$$

▌

命题 4 设 φ 是环 $(R,+,\cdot)$ 到环 $(S,\#,\odot)$ 的同态映射,ψ 是 $(S,\#,\odot)$ 到环 $(K,*,\Delta)$ 的同态映射.那么复合映射 $\psi\circ\varphi$ 是 $(R,+,\cdot)$ 到 $(K,*,\Delta)$ 的环同态映射.

证明 复合映射 $\psi\circ\varphi$ 是群 $(R,+)$ 到群 $(K,*)$ 的群同态映射.同时,对任意 $a,b\in R$,有

$$\begin{aligned}
&(\psi\circ\varphi)(a\cdot b)\\
&=\psi[\varphi(a\cdot b)] && (\text{复合映射的定义})\\
&=\psi[\varphi(a)\odot\varphi(b)] && (\varphi\text{ 是同态映射})
\end{aligned}$$

$$= \psi(\varphi(a)) \Delta \psi(\varphi(b)) \qquad (\psi \text{ 是同态映射})$$
$$= (\psi \circ \varphi)(a) \Delta (\psi \circ \varphi)(b). \qquad (\text{复合映射的定义})$$

这就证明了 $\psi \circ \varphi$ 还是环同态,可画交换图如图 4－3. ▌

命题 5 设 φ 是环$(R, +, \cdot)$到环$(S, \#, \odot)$的同态映射.那么 φ 的核 $\text{Ker}(\varphi)$必然是环 R 的理想.

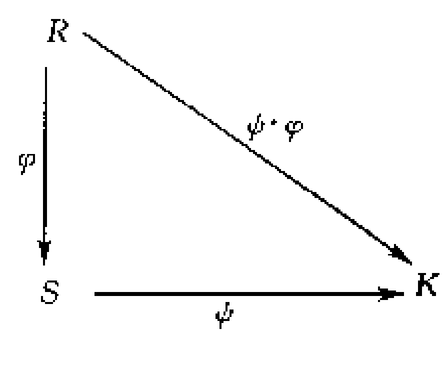


图 4－3

证明 核 $\text{Ker}(\varphi)$也是 φ 作为群$(R, +)$到群$(S, \#)$的群同态的核.所以 $\text{Ker}(\varphi)$首先是群$(R, +)$的子群.

进一步,对任意 $r \in \text{Ker}(\varphi)$, $a \in R$,有
$$\varphi(a \cdot r) = \varphi(a) \odot \varphi(r) = \varphi(a) \odot 0 = 0.$$
同理可得 $\varphi(r \cdot a) = 0$.故 $a \cdot r \in \text{Ker}(\varphi)$, $r \cdot a \in \text{Ker}(\varphi)$, $\text{Ker}(\varphi)$是 R 的理想. ▌

推论 同态映射 φ 为单射的充分必要条件是 $\text{Ker}(\varphi) = \{0\}$.

这是因为环同态当然也是加群同态.用群论的结论即可推得. ▌

命题 6 如果 A 是环 R 的理想,那么
$$\varphi: r \to r + A$$
是环 R 到环 R/A 的满的同态映射.

证明 $(R, +, \cdot)$是个环,$(A, +, \cdot)$是它的理想,作为群来看,在第三章,我们已知道
$$\varphi: a \to a + A$$
是$(R, +)$到商群 R/A 的群同态映射,而且是个满射.进一步,把 R 和 R/A 作为环,看他们的乘法,还有
$$\varphi(ab) = ab + A \qquad (\varphi \text{ 的定义})$$
$$= (a + A)(b + A) \qquad (R/A \text{ 中乘法定义})$$
$$= \varphi(a)\varphi(b) \qquad (\varphi \text{ 的定义})$$
所以,映射 φ 还是满的环同态映射. ▌

命题 6 中建立的 R 到 R/A 的映射 φ 通常称为 R 到 R/A 的自然映射.

定理 设 f 是环 $(R,+,\cdot)$ 到环 $(S,\#,\odot)$ 的满的环同态映射, $\mathrm{Ker}(f)=A$. 那么 R/A 同构于环 $(S,\#,\odot)$.

证明 首先, f 是群 $(R,+)$ 到群 $(S,\#)$ 的满的群同态映射. 由第三章 §4 的关于群的同态基本定理的证明, 可以看到

$$\varphi: a+A \to f(a)$$

是群 R/A 到群 S 的映射, 它与陪集 $a+A$ 的代表元选择无关.

进而还知道 φ 是群 R/A 到群 $(S,\#)$ 的群同态映射.

同时, φ 是满射又是单射.

现在, 我们来看乘法. 有

$$\begin{aligned}
&\varphi[(a+A)(b+A)] \\
&= \varphi(a\cdot b+A) && (R/A \text{ 中乘法定义}) \\
&= f(a\cdot b) && (\varphi \text{ 的定义}) \\
&= f(a)\odot f(b) && (f \text{ 是环同态}) \\
&= \varphi(a+A)\odot\varphi(b+A). && (\varphi \text{ 的定义})
\end{aligned}$$

也就是说, 对任意 $a+A, b+A\in R/A$ 恒有

$$\varphi[(a+A)(b+A)]=\varphi(a+A)\odot\varphi(b+A).$$

φ 是 R/A 到 S 的环同态映射, 而且是个双射, 即 φ 是同构映射, R/A 同构于 S. ▌

通常把命题 6 和上面的定理合起来称为**环同态基本定理**. 它充分反映了环的同态与环的理想的内在联系, 它有许多重要应用, 是进一步学习和研究环理论的基础.

我们看些例子.

例 5 本节例 1, 实系数多项式环 P 到实数环 $\mathbf{R}$ 的映射

$$\varphi: f(x)\to f(a)$$

是个满的同态映射. 且

$$\mathrm{Ker}(\varphi)=\{g(x)\in P \mid g(a)=0\},$$

由同态基本定理, 得 $P/\mathrm{Ker}(\varphi)\cong\mathbf{R}$ (4)

在§3的例3中已经知道

$$\mathrm{Ker}(\varphi)=\{g(x)\in P \mid x-a \text{ 整除 } g(x)\}.$$

如果再看 $(x-a)$ 在 P 中生成的理想 $((x-a))$. 那么,任意 $g(x)\in \mathrm{Ker}(\varphi)$, $x-a$ 整除 $g(x)$,必有 $q(x)\in P$ 使 $g(x)=(x-a)q(x)$,从而

$$g(x)\in((x-a)).$$

反之,若 $g(x)\in((x-a))$,由于 P 是有恒等元的交换环,可设

$$g(x)=k(x-a)+h(x)(x-a)+(x-a)l(x)$$
$$+\sum_{i=1}^{t}q_i(x)(x-a)r_i(x),$$

它可以合并成 $g(x)=q(x)(x-a)$. 这说明 $g(a)=0$, $g(x)\in \mathrm{Ker}(\varphi)$. 所以,$\mathrm{Ker}(\varphi)=((x-a))$. 同构式(4)就是

$$P/((x-a))\cong \mathbf{R}.$$

例6 把本节例2之 $n=3$ 的 n 换成任意正整数. 建立整数环 $\mathbf{I}$ 到 $\mathbf{I}_n$ 的映射 φ,对任意 $m\in \mathbf{I}$,用 n 除 m,

$$m=nq+r,\ 0\leqslant r<n,\quad \varphi: m\to r^*.$$

则 φ 是 $\mathbf{I}$ 到 $\mathbf{I}_n$ 的满的同态映射.

计算

$$\mathrm{Ker}(\varphi)=\{\cdots,-n,0,n,\cdots\}=(n).$$

由环的同态基本定理,得

$$\mathbf{I}/(n)\cong \mathbf{I}_n. \tag{5}$$

我们在前面曾把 $\mathbf{I}$ 对 (n) 的商集写成 $\mathbf{I}_{\sim n}$ 或 $\bar{\mathbf{I}}_n$,元素分别记为[0],[1],…,[$n-1$]. 故(5)也就是 $\mathbf{I}_{\sim n}\cong \mathbf{I}_n$, $\bar{\mathbf{I}}_n\cong \mathbf{I}_n$.

例7 在所有实的2阶矩阵构成的环 $M_{2\times 2}$ 中,子环

$$R=\left\{k\in M_{2\times 2} \mid K=\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}\right\},$$

$$S=\left\{H\in M_{2\times 2} \mid H=\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}\right\}.$$

如同本节之例3所示,映射

$$\varphi:\begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \to \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

是 R 到 S 的环同态映射，而且是满的

$$\mathrm{Ker}(\varphi)=\left\{L\in M_{2\times 2}\,\middle|\, L=\begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix}\right\}.$$

由同态基本定理，知 $R/\mathrm{Ker}(\varphi)\cong S$.

例 8 本节例 4，φ 是 I_4 到 I_2 的满的同态映射，且

$$\mathrm{Ker}\varphi=\{0^*,2^*\}.$$

由环同态基本定理，得 $\mathrm{I}_4/\{0^*,2^*\}\cong\mathrm{I}_2$.

例题 1 设 $(R,+,\cdot)$ 和 $(S,\#,\odot)$ 都是环. f 是 R 到 S 的满的环同态映射，$\mathrm{Ker}(f)=A$. 再设

$$\gamma: r\to r+A$$

是 R 到 R/A 的自然同态. 那么，基本定理证明中建立的 R/A 到 S 的同构映射 φ，

$$\varphi: r+A\to f(r)$$

恰好使得 $f=\varphi\circ\gamma$，也就是下面的图 4－4 可交换

图 4－4

证明 在第三章 §4 中，作为例题，我们已经看到，对任意 $a\in R$，恒有

$$(\varphi\circ\gamma)(a)=f(a).$$

也就是 $f=\varphi\circ\gamma$. 不过，那里的 f,φ 和 γ 都是加法群的群同态映射. 现在，给出的 f 和 γ 都是环的同态映射，又证明了 φ 也是环的同态映射，得到的 $f=\varphi\circ\gamma$ 就是环同态映射的等式了. ▍

例题 2 设 φ 是环 R 到 S 的一个同态映射. 如果 B 是环 S 的一个理想，那么 B 的原像

$$\varphi^{-1}(B)=\{r\in R\mid \varphi(r)\in B\}$$

非空，而且是 R 的一个理想.

证明 任取 $x,y\in\varphi^{-1}(B)$，即 $\varphi(x),\varphi(y)\in B$. 由于 B 是 S

的理想，故 $\varphi(x)-\varphi(y)\in B$；从而

$$\varphi(x-y)=\varphi(x)-\varphi(y)\in B,$$

$x-y\in\varphi^{-1}(B)$. 任取 $x\in\varphi^{-1}(B)$，$r\in R$. 由于 $\varphi(x)\in B$，B 是理想，必有 $\varphi(r)\varphi(x)\in B$；从而

$$\varphi(rx)=\varphi(r)\varphi(x)\in B,$$

$rx\in\varphi^{-1}(B)$. $\varphi^{-1}(B)$是 R 的理想. ∎

下面介绍我国数学家华罗庚证明过的一个有趣的题目.

例题 3′ 设 R 是个环，σ 是 R 到 R 的一个变换，对任意 $a,b\in R$ 恒有

$$\sigma(a+b)=\sigma(a)+\sigma(b),$$

而且，任意取定一组 $x,y\in R$，$\sigma(xy)$只有两种可能

$$\sigma(xy)=\sigma(x)\sigma(y)\text{或 }\sigma(xy)=\sigma(y)\sigma(x).$$

那么，，对所有组 $u,v\in R$ 而言，必然全体一律满足

$$\sigma(uv)=\sigma(u)\sigma(v),$$

或者，全体一律满足 $\sigma(uv)=\sigma(v)\sigma(u)$.

分析 首先要把题意弄清楚. 条件是对任意取定的一对元素 $x,y\in R$，均必有

$$\sigma(xy)=\sigma(x)\sigma(y)\text{或 }\sigma(xy)=\sigma(y)\sigma(x),$$

当然也可能两个等式同时成立. 如果另外再取一对元素 $s,t\in R$，它们亦会有

$$\sigma(st)=\sigma(s)\sigma(t)\text{或 }\sigma(st)=\sigma(t)\sigma(s),$$

当然也有两式同时成立的可能.

这个条件，表面上看，很可能出现这样的情形，即

$$\sigma(xy)=\sigma(x)\sigma(y),\quad \sigma(xy)\neq\sigma(y)\sigma(x),$$

$$\sigma(st)=\sigma(t)\sigma(s),\quad \sigma(st)\neq\sigma(s)\sigma(t).$$

即并非“全体一律”的情形. 我们就是要否定这种情形的出现.

证明 用反证法. 如果两种“全体一律”情形均不对，必然有 $x,y\in R$ 和 $s,t\in R$ 使

$$\sigma(xy)=\sigma(x)\sigma(y),\quad \sigma(xy)\neq\sigma(y)\sigma(x),$$

$$\sigma(st)=\sigma(t)\sigma(s),\quad \sigma(st)\neq\sigma(s)\sigma(t). \tag{6}$$

现在看 $\sigma[(s+x)y]$，由所给条件，应有

$$\sigma[(s+x)y]=\sigma(s+x)\sigma(y)=\sigma(s)\sigma(y)+\sigma(x)\sigma(y),$$

或者

$$\sigma[(s+x)y]=\sigma(y)\sigma(s+x)=\sigma(y)\sigma(s)+\sigma(y)\sigma(x).$$

如果是 $\sigma[(s+x)y]=\sigma(s)\sigma(y)+\sigma(x)\sigma(y)$，由于

$$\sigma[(s+x)y]=\sigma(sy)+\sigma(xy),\quad \sigma(xy)=\sigma(x)\sigma(y),$$

知道必有

$$\sigma(sy)=\sigma(s)\sigma(y). \tag{7}$$

如果是 $\sigma[(s+x)y]=\sigma(y)\sigma(s)+\sigma(y)\sigma(x)$，由于已知

$$\sigma(xy)\neq\sigma(y)\sigma(x),$$

必得 $\sigma(sy)\neq\sigma(y)\sigma(s)$，也必有

$$\sigma(sy)=\sigma(s)\sigma(y).$$

同理可证，

$$\sigma(xt)=\sigma(x)\sigma(t). \tag{8}$$

讨论 $\sigma[s(t+y)]$和 $\sigma[(s+x)t]$又得

$$\sigma(sy)=\sigma(y)\sigma(s),\quad \sigma(xt)=\sigma(t)\sigma(x).$$

最后，看 $\sigma[(x+s)(y+t)]$，有

$$\begin{aligned}
&\sigma(xy+sy+xt+st)\\
&=\sigma(xy)+\sigma(sy)+\sigma(xt)+\sigma(st) && \text{(题设)}\\
&=\sigma(x)\sigma(y)+\sigma(s)\sigma(y)+\sigma(x)\sigma(t)+\sigma(t)\sigma(s) && \text{(见(6),(7),(8))}\\
&\neq\sigma(x)\sigma(y)+\sigma(s)\sigma(y)+\sigma(x)\sigma(t)+\sigma(s)\sigma(t) && (\sigma(t)\sigma(s)\neq\sigma(s)\sigma(t))\\
&=\sigma(x+s)\sigma(t+y),
\end{aligned}$$

即 $\sigma[(x+s)(y+t)]\neq\sigma(x+s)\sigma(t+y)$. 同理，又必有

$$\sigma[(x+s)(y+t)]\neq\sigma(y+t)\sigma(x+s).$$

这与题设矛盾. ▌

例题 4 在实数域 **R** 上 4 阶全阵环 $M_{4\times4}(\mathbf{R})$中，所有形如

$$A=\begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \qquad (*)$$

的矩阵的集合记为 S'.

先来说明：S' 是 $M_{4\times4}(\mathbf{R})$ 的一个子环. 看其中 4 个矩阵

$$I_4=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad I=\begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$J=\begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad K=\begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

由于对任意 $A\in S'$ 如 $*$，恒有

$$A=aI_4+bI+cJ+dK,$$

所以，S' 对矩阵减法是封闭的. 注意到 I_4,I,J,K 的乘法表

	I_4	I	J	K
I_4	I_4	I	J	K
I	I	$-I_4$	K	$-J$
J	J	$-K$	$-I_4$	I
K	K	J	$-I$	$-I_4$

容易看出 S' 对矩阵乘法也是封闭的. 所以，S' 是个环.

进一步，证明：环 S' 同构于 §2 例题 2 中的环 S，S 是所有形如

$$\begin{pmatrix} a+b\sqrt{-1} & c+d\sqrt{-1} \\ -c+d\sqrt{-1} & a-d\sqrt{-1} \end{pmatrix}, \quad a,b,c,d\in\mathbf{R}$$

的复矩阵构成的环.

证明 对任意 $A\in S$ 如(*)，必可唯一地表成

$$A=aI_4+bI+cJ+dK.$$

令

$$\varphi: A\to ae+bi+cj+dk,$$

即得 S' 到 S 的一个映射. 这是个双射. 由于 $\{e,i,j,k\}$ 和 $\{I_4,I,J,K\}$ 有完全一致的乘法表，就不难验证，对任意 $A,B\in S'$ 必有

$$\varphi(AB)=\varphi(A)\varphi(B).$$

而 $\varphi(A+B)=\varphi(A)+\varphi(B)$ 极为显然. 所以，φ 是 S' 到 S 的一个同构映射. ∎

如同在群论中讨论过的那样，我们也可以把一个环 R 到一个集合 S 上的(集合的)双射"加工"成环到环的同构.

例题 5 设 $(R,+,\cdot)$ 是个环，S 是个集合，φ 是 R 到 S 的一个双射，φ^{-1} 是 φ 的逆映射. 那么，对任意 $a,b\in S$，规定

$$a\#b=\varphi[\varphi^{-1}(a)+\varphi^{-1}(b)],$$

$$a\odot b=\varphi[\varphi^{-1}(a)\cdot\varphi^{-1}(b)],$$

则 $(S,\#,\odot)$ 是个环，φ 是环 $(R,+,\cdot)$ 到环 $(S,\#,\odot)$ 的环同构映射.

证明 首先应注意到，任取 $a,b\in S$，由于 φ 是双射，故有确定的 $\varphi^{-1}(a)$，$\varphi^{-1}(b)\in R$，而 R 是环，$\varphi^{-1}(a)+\varphi^{-1}(b)$ 和 $\varphi^{-1}(a)\cdot\varphi^{-1}(b)$ 都是 R 中的确定的元素. 从而

$$\varphi[\varphi^{-1}(a)+\varphi^{-1}(b)],\quad \varphi[\varphi^{-1}(a)\cdot\varphi^{-1}(b)]$$

都是 S 中确定的元素. 故 $\#$ 和 $\odot$ 是 S 上的两个二元运算.

要验证各种算律都极容易. 仅以分配律为例说明一下.

任取 $a,b,c\in S$，必有

$$\begin{aligned}
&(a\#b)\odot c\\
&=\varphi\{\varphi^{-1}(a\#b)\cdot\varphi^{-1}(c)\} && (\odot\text{的定义})\\
&=\varphi\{\varphi^{-1}\varphi[\varphi^{-1}(a)+\varphi^{-1}(b)]\cdot\varphi^{-1}(c)\} && (\#\text{的定义})\\
&=\varphi\{[\varphi^{-1}(a)+\varphi^{-1}(b)]\cdot\varphi^{-1}(c)\} && (\varphi^{-1}\varphi\text{ 为恒等映射})\\
&=\varphi\{\varphi^{-1}(a)\cdot\varphi^{-1}(c)+\varphi^{-1}(b)\cdot\varphi^{-1}(c)\} && (R\text{ 满足分配律})
\end{aligned}$$

$$=\varphi\{\varphi^{-1}\varphi[\varphi^{-1}(a)\cdot\varphi^{-1}(c)]+\varphi^{-1}\varphi[\varphi^{-1}(b)\cdot\varphi^{-1}(c)]\}$$
（$\varphi^{-1}\varphi$ 为恒等映射）

$$=\varphi\{\varphi^{-1}(a\odot c)+\varphi^{-1}(b\odot c)\}$$ （$\odot$的定义）

$$=a\odot c\# b\odot c.$$ （#的定义）

若 $0'$ 是 R 的零元素，则 $\varphi(0')=0$ 必为 S 的零元素. 因为，对任意 $a\in S$，必有

$$a\#0=\varphi[\varphi^{-1}(a)+\varphi^{-1}(0)]$$ （#的定义）
$$=\varphi[\varphi^{-1}(a)+0']$$ （$\varphi(0')=0$）
$$=\varphi[\varphi^{-1}(a)]$$ （$0'$ 是 R 的零元）
$$=a.$$ （$\varphi\varphi^{-1}$ 是恒等映射）

又，对任意 $a\in S$，$\varphi[-\varphi^{-1}(a)]$ 必为 a 的负元，这是因为

$$a\#\varphi[-\varphi^{-1}(a)]$$
$$=\varphi\{\varphi^{-1}(a)+\varphi^{-1}\varphi[-\varphi^{-1}(a)]\}$$ （#的定义）
$$=\varphi\{\varphi^{-1}(a)+-\varphi^{-1}(a)\}$$ （$\varphi^{-1}\varphi$ 是恒等映射）
$$=\varphi(0')$$ （$-\varphi^{-1}(a)$ 是 $\varphi^{-1}(a)$ 的负元）
$$=0.$$

所以，$(S,\#,\odot)$ 是个环.

对任意 $a',b'\in R$，设 $\varphi(a')=a$，$\varphi(b')=b$，则

$$\varphi(a'+b')$$
$$=\varphi[\varphi^{-1}\varphi(a')+\varphi^{-1}\varphi(b')]$$ （$\varphi^{-1}\varphi$ 是恒等映射）
$$=\varphi(a')\#\varphi(b'),$$ （#的定义）

而且也有

$$\varphi(a'\cdot b')$$
$$=\varphi[\varphi^{-1}\varphi(a')\cdot\varphi^{-1}\varphi(b')]$$ （$\varphi^{-1}\varphi$ 是恒等映射）
$$=\varphi(a')\odot\varphi(b').$$ （$\odot$的定义）

这样，我们完整地证明了，φ 是环 $(R,+,\cdot)$ 到环 $(S,\#,\odot)$ 的同构映射. ▌

与此例类似，还有

例题 6 设 $(R,+,\cdot)$ 是个环，集合 S 有两个二元运算 # 和

⊙.如果有集合 R 到集合 S 的满的映射 σ,对任意 $a,b\in R$ 均有

$$\sigma(a+b)=\sigma(a)\#\sigma(b), \tag{9}$$

$$\sigma(a\cdot b)=\sigma(a)\odot\sigma(b), \tag{10}$$

那么 $(S,\#,\odot)$ 必然也是个环.

证明 运算律的验证仍以分配律为例.

任取 $x,y,z\in S$,由于 σ 是满的,必有 $a,b,c\in R$ 使得

$$x=\sigma(a),\quad y=\sigma(b),\quad z=\sigma(c). \tag{11}$$

于是,

$$\begin{aligned}
&(x\# y)\odot z\\
&=[\sigma(a)\#\sigma(b)]\odot\sigma(c) && (\sigma\text{ 是满的})\\
&=\sigma(a+b)\odot\sigma(c) && (\text{见}(10))\\
&=\sigma[(a+b)\cdot c] && (\text{见}(9))\\
&=\sigma(a\cdot c+b\cdot c) && (R\text{ 中分配律})\\
&=\sigma(a\cdot c)\#\sigma(b\cdot c) && (\text{见}(9))\\
&=(\sigma(a)\odot\sigma(c))\#(\sigma(b)\odot\sigma(c). && (\text{见}(10))
\end{aligned}$$

设 $0'$ 是环 R 的加法零元素,$\sigma(0')=\theta\in S$ 必为 $(S,\#)$ 的零元素.这是因为,任取 $x\in S$,设 $x=\sigma(a)$, $a\in R$,则

$$\begin{aligned}
x\#\theta&=\sigma(a)\#\sigma(0') && (\sigma(0')=\theta)\\
&=\sigma(a+0') && (\sigma\text{ 的性质}(9))\\
&=\sigma(a) && (0'\text{是}R\text{ 的零元})\\
&=x.
\end{aligned}$$

对任意 $x\in S$,设 $x=\sigma(a)$,则

$$\begin{aligned}
&x\#\sigma(-a)\\
&=\sigma(a)\#\sigma(-a) && (x=\sigma(a))\\
&=\sigma[a+(-a)] && (\sigma\text{ 的性质}(9))\\
&=\sigma(0') && (-a\text{ 是}a\text{ 在}R\text{ 中的负元})\\
&=\theta.
\end{aligned}$$

所以,$(S,\#)$ 是个加法群.进而,$(S,\#,\odot)$ 还是个环. ▎

此例题虽然证明起来不难,但应用起来却方便,本书第七章中

要用到它.

为说话方便人们常把满的同态映射称为**满同态**,单的同态映射称为**单同态**,而环到自己的同态称为**自同态**(进一步,此同态映射为双射时,称为**自同构**).

例题 7 若整数 m 与整数 18 互素,那么 18 一定能整除

$$m^6-1.$$

证明 按照例 6 的方法建立 $\mathbf{I}$ 到 $\mathbf{I}_{18}$ 的同态映射 φ,对任意 $k\in\mathbf{I}$,

$$k=nq+r,\quad 0\leqslant r<18,$$

则 $\varphi(k)=r^*$.

因为 m 与 18 互素,18 去除 m,余数只能是

$$1,5,7,11,13,17 \tag{1}$$

所以,$\varphi(m)$只能是 $\mathbf{I}_{18}$ 下列元之一

$$1^*,5^*,7^*,11^*,13^*,17^*.$$

若 k 与 18 互素,l 与 18 互素,则 kl 亦与 18 互素. 也就是说,若用 18 除之,k 余 r_1,l 与 r_2,那么 kl 余数亦在(1)式之 6 数中间,由于

$$\varphi(kl)=\varphi(k)\varphi(l)=r_1^*r_2^*\in\{1^*,5^*,7^*,11^*,13^*,17^*\},$$

我们知道$\{1^*,5^*,7^*,11^*,13^*,17^*\}$是乘法封闭的.

再进一步看,还有

$$(5^*)^{-1}=11^*,\quad (7^*)^{-1}=13^*,\quad 17^*\cdot 17^*=1^*,$$

所以,$\{1^*,5^*,7^*,11^*,13^*,17^*\}$在 $\mathbf{I}_{18}$ 的乘法之下是个 6 元群. 由凯莱定理知它的每个元数的 6 次幂均为 1^*.

这说明,只要 m 与 18 互素,则 $\varphi(m)^6=1^*$. 而 φ 是同态映射,故 $\varphi(m^6)=1^*$,也就是 m^6 被 18 除时余 1,

$$18\mid(m^6-1).$$ ▎

习 题 四

1. (见本节之例 3)求环 R 的自同态

$$\sigma:\begin{pmatrix}a & c\\0 & b\end{pmatrix}\to\begin{pmatrix}a & 0\\0 & b\end{pmatrix},\quad a,b,c\text{ 是个实数}$$

的核.令

$$A=\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix},\quad B=\begin{pmatrix}0 & 0\\0 & \pi\end{pmatrix}.$$

求原像 $\varphi^{-1}(\{A\}),\varphi^{-1}(\{B\})$.

2. 设 f,g 都是从有理数环 $\mathbf{Q}$ 到实数环 $\mathbf{R}$ 的同态映射.且对每 $i\in\mathbf{I}$ 恒有 $f(i)=g(i)$.证明:f 和 g 是 $\mathbf{Q}$ 上相同的映射,也就是

$$f(x)=g(x),\quad\text{对所有 } x\in\mathbf{Q}$$

3. 设 f 是环 R 到环 R' 的同态映射,S 是 R 的子环,证明:S 的像 $f(S)$ 是环 R' 的子环.

4. 设 I,J 都是环 R 的理想,规定 $f:x\to x+J$ 得到 I 到环 R/J 的映射.证明:f 是环同态映射,求出 f 的核.

5. 设 T 是所有形如

$$a+b\sqrt{3},\quad a,b\in\mathbf{I}$$

的实数作成的 R 的子环.令

$$f:a+b\sqrt{3}\to a-b\sqrt{3}.$$

证明:f 是 T 的自同态.求出 $\mathrm{Ker}(f),\mathrm{Img}(f)$.

§5* 环的直和

设$(R,+,\cdot)$和$(S,\#,\odot)$都是环.作为集合,在第一章里,讨论了笛卡尔积 $R\times S$,

$$R\times S=\{(r,s)\mid r\in R,\ s\in S\}.$$

由于$(R,+)$和$(S,\#)$都是群,第二章§6又给出一个硬性"拼凑"方法,将集 $R\times S$ 定义成群.

$$(a,x)*(b,y)=(a+b,x\# y).$$

现在,还可以由 R 的乘法$\cdot$和 S 的乘法$\odot$硬性地引出 $R\times S$ 的运算 Δ(仍称为乘法),

$$(a,x)\Delta(b,y)=(a\cdot b,x\odot y).$$

因为 $R\times S$ 的运算完全依靠 R 和 S 的运算，且任何运算规律的验证都等于分别在 R 和 S 中验证相应的规律，读者容易看出

(1) $(R\times S,*)$是个加法群，这是在第二章群论中讲过的；

(2) $(R\times S,\Delta)$满足结合律；

(3) $R\times S$ 的运算 Δ 和 $*$ 满足分配律.

也就是说，$(R\times S,*,\Delta)$是个环. 这个环就称为是环 R 和 S 的**外直和**，记为 $R\oplus S$.

令

$$R'=\{(r,0)\in R\times S,\ r\in R\},$$
$$S'=\{(0,s)\in R\times S,\ s\in S\}.$$

那么，容易看出，R'和 S'均为 $R\oplus S$ 的理想.

对照群的直积，可以看出，$R\oplus S$ 与 R'，S'有如下关系：

(1) R'和 S'均为 $R\oplus S$ 的理想；

(2) $R\oplus S=R'*S'$，即 $R\oplus S$ 的每个元素(r,s)均可表成 R'和 S'元素之和，例如$(r,s)=(r,0)*(0,s)$；

(3) 上述表示法，对每个 $R\oplus S$ 中元素来说，都是唯一确定的；

(4) R'中任意元 x 和 S'中任意元 y 的积 $x\Delta y$ 恒为 0；

(5) $R'\cap S'$仅含 $R\oplus S$ 的零元.

仔细分析一下，这些条件并不是完全独立的. 比如说，只要有前 3 条就可以推出后两条性质. 为此，我们对环与其理想满足前 3 条公理者要特别加以研究.

定义 1 设 R 是个环，A 和 B 是 R 的理想. 如果

(1) $R=A+B$，即对任意 $r\in R$，都有

$$r=a+b,\quad a\in A,\ b\in B,$$

(2) 上述之 R 元表示成 A 元与 B 元之和的表示法是唯一的，那么，说环 R 是其理想 A，B 的**内直和**.

命题 1 对任意环 R 和环 S，其外直和 $R\oplus S$ 必为两理想 R' 和 S'的内直和，其中

$$R'=\{(r,0)\in R\times S\}\simeq R,\quad S'=\{(0,s)\in R\times S\}\cong S.$$ ▌

例 1 所有 2 阶整数对角矩阵构成的环记为 R，且

$$A=\left\{\begin{pmatrix}a&0\\0&0\end{pmatrix}\in R\right\},\quad B=\left\{\begin{pmatrix}0&0\\0&b\end{pmatrix}\in R\right\}.$$

则 R 是理想 A,B 的内直和.

命题 2 设 R 是个环，A 和 B 是 R 的理想. 那么，R 为 A,B 的内直和的充分必要条件是

(1) $R=A+B$;

(2) R 的零元 0 表示成 A 元和 B 元之和时，表示法唯一.

证明 如果 R 是 A,B 的内直和，当然满足条件(1)，同时 R 中任意元表示成 A 元和 B 元之和时，表示法均唯一，当然也就满足(2).

反过来，如果满足(1)，$R=A+B$，且 R 中零元 0 表示成 A 元与 B 元之和时表示法唯一. 那么，对于 R 中的任意元 r，若有

$$r=a+b=c+d,\quad a,c\in A,\ b,d\in B,$$

必导致

$$0=(a-c)+(b-d),\quad a-c\in A,\ b-d\in B.$$

而已知 0 的表示法唯一，只能是 $0=0+0$，所以

$$a-c=0,\quad b-d=0;$$

也就是 $a=c,\ b=d,\ r$ 的表示法唯一. 从而 R 为 A,B 的内直和.

▌

命题 3 设 R 是个环，A 和 B 是 R 的理想. 那么，R 是 A,B 的内直和的充要条件是

(1)′ $R=A+B$;

(2)′ $A\cap B=\{0\}$.

证明 与命题 2 对照，我们只要证明，在 $R=A+B$ 的前提下，(2)和(2)′等价.

如果 $A\cap B=\{0\}$. 而 0 有表示法

$$0=a+b,\quad a\in A,b\in B,$$

则 $a=-b$. 从左端看该元应在 A 中,从右端看该元又应在 B 中,故

$$a=-b\in A\cap B=\{0\};$$

也就是 $a=0$, $b=0$. R 之零元 0 表示法唯一,只有 $0=0+0$.

反之,如果已知 R 中零元 0 表示法唯一,而 $x\in A\cap B$,那么,因为 $A\cap B$ 是理想,又应有 $-x\in A\cap B$. 于是,等式

$$0=x+(-x)$$

中,$x\in A$, $-x\in B$,得到 0 的一个表示法. 据唯一性假定,必有 $x=0$. 即 $A\cap B=\{0\}$. ▌

例 2 研究环

$$\mathbf{I}_6=\{0^*,1^*,2^*,3^*,4^*,5^*\}$$

和它的理想 $A=\{0^*,2^*,4^*\}$, $B=\{0^*,3^*\}$.

由于 $1^*=4^*+3^*\in A+B$,而 $\mathbf{I}_6$ 中任意元都是若干个 1^* 之和,故 $R=A+B$. 进一步,有

$$A\cap B=\{0^*\}.$$

所以 $\mathbf{I}_6$ 是 A 和 B 的内直和.

命题 4 若 R 是其理想 A,B 的内直和,则任意 $a\in A$, $b\in B$ 必有

$$ab=ba=0.$$

从而,对任意

$$x=a+b,\ y=c+d,\quad a,c\in A,\ b,d\in B$$

有 $(a+b)(c+d)=ac+bd$.

证明 因为 R 是 A,B 的内直和,故

$$A\cap B=\{0\}.$$

于是,对任意 $a\in A$, $b\in B$,先由 A 是 R 理想推知 $ab,ba\in A$;再由 B 也是 R 的理想得到 $ab,ba\in B$;最后合起来就有

$$ab,ba\in A\cap B=\{0\},$$

即 $ab=ba=0$.

若 $a,c\in A$, $b,d\in B$,必有 $bc=0$, $ad=0$,从而

$$(a+b)(c+d)=ac+bd.$$ ▌

这个命题反映了环的内直和概念和外直和概念的本质联系.具体说来,有

定理 1 若环 R 是其理想 A,B 的内直和,则 R 同构于 A 和 B 的外直和.

证明 任取 $(a,b)\in A\oplus B$,令

$$\varphi:(a,b)\to a+b.$$

则 φ 是集 $A\times B$ 到 R 的一个映射.且对任意 $(a,b),(c,d)\in A\oplus B$,恒有

$$\begin{aligned}
&\varphi[(a,b)\Delta(c,d)]\\
&\quad=\varphi[(ac,bd)] &&(A\oplus B\text{ 中乘法 }\Delta\text{ 的定义})\\
&\quad=ac+bd &&(\varphi\text{ 的定义})\\
&\quad=(a+b)(c+d) &&(\text{命题 }4)\\
&\quad=\varphi[(a,b)]\varphi[(c,d)]. &&(\varphi\text{ 的定义})
\end{aligned}$$

同时还有

$$\begin{aligned}
&\varphi[(a,b)*(c,d)]\\
&\quad=\varphi[(a+c,b+d)] &&(A\oplus B\text{ 中加法 }*\text{ 的定义})\\
&\quad=(a+c)+(b+d) &&(\varphi\text{ 的定义})\\
&\quad=(a+b)+(c+d) &&(\text{这是 }R\text{ 中加法})\\
&\quad=\varphi[(a,b)]+\varphi[(c,d)]. &&(\varphi\text{ 的定义})
\end{aligned}$$

所以,φ 是 $A\oplus B$ 到 R 的环同态映射.

又,环 R 是 A,B 的内直和,任意 $r\in R$ 均可写成 $r=a+b$, $a\in A$, $b\in B$,从而

$$\varphi[(a,b)]=a+b=r,$$

故知 φ 是满射.

再则,若有 $(a,b),(c,d)\in A\oplus B$ 且

$$\varphi[(a,b)]=\varphi[(c,d)],$$

那么,就得到 $a+b=c+d$.但 R 是 A,B 的内直和,表示唯一性蕴涵着 $a=c$, $b=d$,即

$$(a,b)=(c,d),$$

这说明 φ 是个单射.

总之,φ 是 $A\oplus B$ 到 R 的环同构映射. ∎

正是因为环的外直和与内直和有命题 1 和定理 1 这样同构性的事实,如同在群的讨论中一样,有些书对它们不加区分,使用相同符号和术语.读者刚刚开始接触这类概念,要特别加以注意.

例题 1 若环 R 是其理想 A,B 的内直和,则 $R/A\cong B$.

证明 对任意 $r\in R$,由于 R 是 A,B 的内直和,所以有 $a\in A$, $b\in B$ 使

$$r=a+b,$$

而且 b 是由 r 唯一确定的.规定

$$\varphi: r\to b$$

就得到了 R 到 B 的一个映射.

对任意 $x,y\in R$,设

$$x=a+b,\quad a\in A,\ b\in B,$$
$$y=c+d,\quad c\in A,\ d\in B.$$

那么

$$x+y=(a+c)+(b+d),\quad a+c\in A,\ b+d\in B,$$

从而 $\varphi(x+y)=b+d=\varphi(x)+\varphi(y)$.同时

$$xy=(a+b)(c+d)=ac+bd,\quad ac\in A,\ bd\in B.$$

故 $\varphi(xy)=bd=\varphi(x)\varphi(y)$.这就是说,$\varphi$ 是个环同态映射.

对任意 $b\in B$,都有 $\varphi(0+b)=\varphi(b)=b$,即 φ 为满射.

又,若 $x\in R$, $x\in \mathrm{Ker}(\varphi)$, $\varphi(x)=0$,则必有 $x\in A$.同时,任意 $a\in A$ 都有 $\varphi(a)=\varphi(a+0)=0$,所以,$\mathrm{Ker}(\varphi)=A$.据环同态基本定理

$$R/A\cong B.$$ ∎

例题 2 设环 R 是其理想 $A_1,\cdots,A_n$ 的内直和,且 R 有恒等元.证明:每个环 A_i 必有恒等元.进一步,R 的元素 a 表成

$$a=a_1+\cdots+a_n,\quad a_i\in A_i$$

后，a 为 R 的一个单位的充分必要条件是诸 a_i 各是环 A_i 的单位.

证明 设 e 是环 R 的恒等元. 由于 A 是诸 A_i 的内直和，必有 $e_i \in A_i$ 使

$$e = e_1 + e_2 + \cdots + e_n.$$

现可断言，e_1 是环 A_1 的一个单位. 任取 $a_1 \in A_1$，因为 e 是大环 R 的恒等元，故 $ea_1 = a_1 e$. 由命题 4 又知 $a_1 e_i = e_i a_1 = 0$，对 $i = 2, \cdots, n$ 都成立. 所以

$$ea_1 = a_1 e = a_1 e_1 + \cdots + a_1 e_n = a_1 e_1 = e_1 a_1 = a_1.$$

由 a_1 的任意性即知 e_1 是环 A_1 的恒等元. 同理，$e_2, \cdots, e_n$ 分别是 $A_2, \cdots, A_n$ 的恒等元.

若 $a \in A$，a 是 A 的单位，

$$a = a_1 + \cdots + a_n, \quad a_i \in A_i, \ i = 1, 2, \cdots, n.$$

设有 $b \in A$，$ab = ba = e$，

$$b = b_1 + \cdots + b_n, \quad b_j \in A_j, \ j = 1, 2, \cdots, n.$$

由命题 4 可得

$$e = ab = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n.$$

但，我们已设

$$e = e_1 + e_2 + \cdots + e_n,$$

由表示法唯一性，必得

$$a_1 b_1 = e_1, a_2 b_2 = e_2, \cdots, a_n b_n = e_n.$$

同理，还有

$$b_1 a_1 = e_1, \ b_2 a_2 = e_2, \ \cdots, \ b_n a_n = e_n.$$

这就说明，$a_1, \cdots, a_n$ 分别是 $A_1, \cdots, A_n$ 的单位. ▌

习 题 五*

1. 若环 R 和环 S 都是可交换的，则它们的外直和 $R \oplus S$ 也是可换环.

2. 若环 R 和环 S 的每个元素都是加法周期有限的，则它们的外直和每个元也都是加法周期有限的.

3. 若环 R 和环 S 的每个元素都是幂零的，则它们的外直和 $R\oplus S$ 的每个元素也都是幂零的.

4. 设 I,J 是环 R 的两个理想. 现建立环 R 到环 $(R/I)\oplus(R/J)$ 的映射

$$f: r \to (r+I, r+J), \quad r\in R.$$

证明：f 是个环同态，并求出 $\mathrm{Ker}(f)$.

小　结

若 $(R,+,\cdot)$ 是个环，那么首先 $(R,+)$ 是个加法群；若 $(S,+,\cdot)$ 是环 $(R,+,\cdot)$ 的子环，那么首先 $(S,+)$ 是加法群 $(R,+)$ 的子群；若 f 是环 $(R,+,\cdot)$ 到环 $(R',\#,\odot)$ 的环同态映射，那么首先 f 是群 $(R,+)$ 到群 $(R',+)$ 的群同态映射. 所以，讨论环的基本性质、子环的结构、环同态映射的作用时，我们首先要想到，在第二、三章群论学习中，已经作了相当的准备，要尽量利用已经掌握了的知识.

例如，讨论环同态映射 f 是否为单射，可以用核 $\mathrm{Ker}(f)$ 是否为零来判断. 而 f 作为环同态映射或单单作为加法群的群同态映射核是相同的. 于是，可以把学习群论时得到的关于核的计算公式、方法完全照搬到环上来.

当然，环 $(R,+,\cdot)$ 有两个二元运算，这两个运算不是井水不犯河水、各行其是，它们是密切配合在一起的. 而联系的渠道就是分配律，及由此得到的一些简单性质，如对任意元素 a,b 恒有

$$a\cdot 0=0, \quad a\cdot(-b)=-(a\cdot b).$$

环中的零元 0 是对于加法运算来说的一个特殊的元素，但它在乘法之下也有独特作用. 所以，环理论中很注重"零因子"的出现. 它也是抽象环比数环概括性更强的一个重要标志. 由零因子、幂零元的存在而引起了环论中一些相当重要的课题研究.

本章的重点是理想、同态和商环.

本章的难点，对某些读者来说，是商环. 如果，在前三章的学习中，你对商集、商群的元素表示方法、定义映射时验证合理性之必

要等已经搞清弄懂，一般来说，对引入商环这一概念不应感到突然.

如果$(I,+)$是环$(R,+,\cdot)$的加法子群，就可以考虑商群$(R,+)/(I,+)$.但想使这个商群能利用$(R,+,\cdot)$的乘法自然的构造成环，I在R的加法和乘法之下构成子环是不够的.这样才引进了环的理想这一重要概念.而且，你一定要体会这么一点味道：理想的引进是相当自然的.

也有可能有些读者到现在对商群甚至商集还不熟悉，那么，你一定不要怕费时间，要按第二章小结建议的办法从头复习一遍.要知道，关于商集、商群和商环的学习是本课程最重要的环节之一，躲是躲不过去的.

复 习 题

1. 在有理数环$(\mathbf{Q},+,\cdot)$中给出

(a) $\frac{1}{2}$在$(\mathbf{Q},+)$中生成的子群；

(b) $\frac{1}{2}$在$(\mathbf{Q}-\{0\},\cdot)$中生成的子群；

(c) $\frac{1}{2}$在$(\mathbf{Q},+,\cdot)$中生成的子环；

(d) $\frac{1}{2}$在$(\mathbf{Q},+,\cdot)$中生成的理想.

2. 设R是所有以整数为系数的多项式所构成的环.证明：由$\{2,x\}$生成的理想$(2,x)$不能是R的主理想；也就是说，$(2,x)$不可能是由R中某一个多项式生成的理想.

3. 设S是环R的子环，则

$$T=\{r\in R\mid rs=sr\text{ 对所有 }s\in S\}$$

是R的子环.

4. 设I是环R的理想，那么$T=\{r\in R\mid rx=0\text{ 对所有 }x\in I\}$是$R$的理想.

5*. 设I是环R的理想，那么

$$T=\{r\in R\mid rx\in I\text{ 对所有 }x\in \mathbf{I}\}$$

是环 R 的理想.

6. 在有理数环($\mathbf{Q}$, +, ·)中

$$S=\{2m/n \mid n\neq 0,\ (m,n)=1,\ m,n\in \mathbf{I}\}$$

是不是子环？是不是理想？

7. 设 p 是个素数，找出商环 $\mathbf{I}/(p^2)$的所有单位和所有幂零元.

8. 条件如上题，给出商环 $\mathbf{I}/(p^2)$的所有非平凡理想

9. 设 D 是个整环，e 是它的恒等元. 且 $e+e+e+e=0$. 证明：$e+e=0$.

10. 若环 R 有 4 个元素$\{0,e,a,b\}$，其中 e 为 R 的恒等元，且元素 a,b 都是单位，给出 R 的乘法表.

11. 若环 R 有 4 个元素$\{0,e,a,b\}$，其中 e 为 R 的恒等元，又知道 $e+e=a$，给出 R 的加法表和乘法表.

12. 利用 $\mathbf{I}$ 到 $\mathbf{I}/(3)$的自然同态映射说明方程 $x^2-3y^2=992$ 没有整数解.

13*. 利用 $\mathbf{I}$ 到 $\mathbf{I}/(17)$的自然同态映射，证明：方程 $x^2-17y^2=855$ 没有整数解.

第五章　从环到域

在我们已经见过的各种环中在结构上存在着很大的差别. 也就是说,尽管这些代数系统都满足环的定义中要求的几条公理,但它们的代数运算仍然有相当大的差异.

例如,整数环 $\mathbf{I}$ 是环论讨论的主要背景之一,它有乘法恒等元,可交换,没有非零的零因子.

而所有实的 $n\times n$ 矩阵构成的环 $M_{n\times n}$,也是环论的重要研究对象,它却既不可换,又不是无零因子环.

甚至,环 $\mathbf{I}_5$ 和 $\mathbf{I}_6$ 表面上运算规律基本相同,元素个数仅差一个,而实际上,从环同构的观点看,它们是完全不同类型的环. 环

$$\mathbf{I}_6=\{0^*,1^*,2^*,3^*,4^*,5^*\}$$

有 2 个非平凡理想

$$A=\{0^*,2^*,4^*\},\quad B=\{0^*,3^*\}.$$

I_6 是 A,B 的内直和,它好像是一个二元环和一个三元环硬拼凑起来的. 但是,环

$$\mathbf{I}_5=\{0^*,1^*,2^*,3^*,4^*\}.$$

除$\{0^*\}$和本身外无任何其他理想,各元素之间关系"紧密",非零元在乘法之下构成群.

本章主要讨论几种环的重要类型及各类型的关系与转换.

§1　除环和域

定义 1　设$(R,+,\cdot)$是个至少含 2 个元素的环. 用 R_0 代表

R 中所有非零元的集合. 如果 R_0 在 R 的乘法·之下是个群, 则说环$(R, +, \cdot)$是个**除环**. 进一步, 若$(R, +, \cdot)$是交换环, 又是除环, 则说$(R, +, \cdot)$是个**域**.

有人称除环为**体**、**除体**、**斜域**. 有人称域为交换除环或交换体.

例如, 有理数环、实数环、复数环都是域, 当然也是除环.

例 1 环 $\mathbf{I}_5$ 是个域. 1^* 是它的乘法恒等元, 且

$$1^* \cdot 1^* = 2^* \cdot 3^* = 4^* \cdot 4^* = 1^*,$$

即每个非零元都有乘法逆元素, $\{1^*, 2^*, 3^*, 4^*\}$构成一个乘法群. $\mathbf{I}_5$ 是交换的除环, 也就是域.

例题 1 先复习一下第四章 §2 之例题 2. S 是所有形如

$$x = \begin{pmatrix} a + b\sqrt{-1} & c + d\sqrt{-1} \\ -c + d\sqrt{-1} & a - b\sqrt{-1} \end{pmatrix}, \quad a, b, c, d \text{ 为实数}$$

的矩阵的集合在矩阵加法和乘法之下构成的环.

矩阵

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

是 S 的乘法恒等元.

计算矩阵 x 的行列式, 得

$$\begin{vmatrix} a + b\sqrt{-1} & c + d\sqrt{-1} \\ -c + d\sqrt{-1} & a - b\sqrt{-1} \end{vmatrix} = a^2 + b^2 + c^2 + d^2,$$

所以, 只要 x 不是零矩阵, 即实数 a, b, c, d 不全为 0, x 的行列式即不为 0, 从而 x 必为可逆矩阵. 设 $a^2 + b^2 + c^2 + d^2 = \delta$, x 的逆矩阵

$$y = x^{-1} = \begin{pmatrix} \dfrac{a - b\sqrt{-1}}{\delta} & \dfrac{-c - d\sqrt{-1}}{\delta} \\ \dfrac{c - d\sqrt{-1}}{\delta} & \dfrac{a + b\sqrt{-1}}{\delta} \end{pmatrix},$$

而且 x^{-1} 也是 S 中的元素. 换言之, S 中有元素 y 使得

$$xy=yx=e.$$

S 中所有非零元做成一个乘法群. ∎

S 是个除环. 这是除环的一个重要例子,称为**四元数(除)环**或**哈密尔顿(Hamilton)四元数环**.

从第四章例题中的乘法表上可以清楚地看出,四元数除环乘法不是可换的. 所以,它不是个域.

给定一个环$(R,+,\cdot)$,要验证$(R_0,\cdot)$是个群,并不需要真的去检验乘法的结合律,因为环 R 的乘法有结合律,R_0 是 R 的子集,R_0 对乘法当然也有结合律,故有以下等价的

定义 2 设$(R,+,\cdot)$是个至少含 2 个元素的环 如果

(1) R 有乘法恒等元 1;

(2) 对任意 $r\in R$,只要 $r\neq 0$,则必有 $s\in R$ 使得

$$rs=sr=1.$$

则说环$(R,+,\cdot)$是个**除环**.

当然,条件(2)又可以换成"R 的非零元恒有乘法逆元"等等.

今后,我们将"乘法恒等元"简称为恒等元. 在不发生混淆时,一律记成"1",有恒等元的环也简单也说成是有 1 环. 读者要注意,1 并不永远代表"数".

而对于加法运算之下的恒等元,我们称为零元,记为 0,前面已经这样做了.

定义 1 和定义 2 的等价性的证明 如果环 R 的所有非零元的集合 R_0 在 R 的乘法之下构成群. 设 e 是群 R_0 的恒等元,即对任意 $r\in R_0$ 必有

$$er=re=r.$$

但 R 与 R_0 仅差一个零元素 0,且

$$e\cdot 0=0\cdot e=0,$$

所以,对任意 $x\in R$,都有 $ex=xe=x$, e 为整个环R 的恒等元,R 满足条件(1).

对任意 $r\in R$，只要 $r\neq 0$，则 $r\in R_0$. 而 R_0 是群，必有 $s\in R_0\subseteq R$ 使得

$$sr=rs=e,$$

即 R 满足条件(2).

反之，假设环 R 满足条件(1)和条件(2). 首先，任意 $x,y\in R_0$，则必有 $xy\in R_0$，即 $xy\neq 0$. 若不然，据条件(1)和条件(2)应有 z 使

$$yz=zy=1,$$

从而导致

$$0=(xy)z=x(yz)=x.$$

这说明 R_0 在 R 的乘法之下封闭. 换言之，环 R 的乘法运算也是 R_0 上的运算.

其次，条件(1)表明 R 有恒等元 1，于是必有 $1\neq 0$. 若不然会导致对任意 x，

$$x=1\cdot x=0\cdot x=0$$

与 R 至少含 2 个元素矛盾. 所以 $1\in R_0$，R_0 有恒等元.

最后，对任意 $r\in R_0$，因为 $r\neq 0$，据条件(2)，必有 $s\in R$，使得

$$rs=sr=1,$$

显然 $s\neq 0$，否则导致 $rs=sr=0$，矛盾. 这说明 $s\in R_0$，即 r 在 R_0 中恒有逆元.

所以，R_0 在乘法之下构成群. ∎

我们看到，环 R 为除环，首先其非 0 元集 R_0 在乘法之下封闭，即 $x,y\in R$ 且 $x\neq 0$，$y\neq 0$ 则必有 $xy\neq 0$. 换言之，R 为无零因子环.

现在问，如果无零因子环 R 至少含两个元，是否 R 为除环呢？

此事显然不对. 比如整数环. 又如，所有实系数多项式构成的环 P 就是无零因子环. 但多项式 x 在 P 中无逆元；因为，对任意一

个 n 次多项式 $f(x)$ 来说，$xf(x)$ 必为 $n+1$ 次多项式，绝不能等于 1.

综上所述，我们可将环的几种重要类型列表如图 5－1.

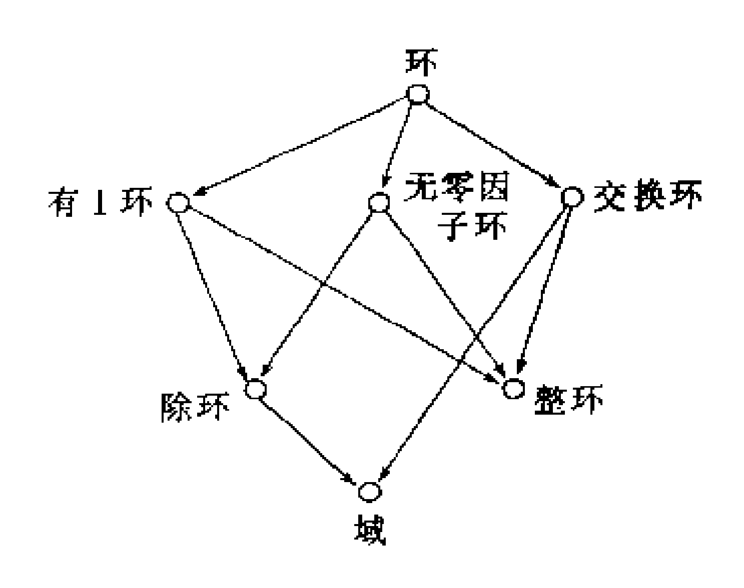


图 5－1

例 2　在实数域 $\mathbf{R}$ 中，子集

$$S=\{x\in\mathbf{R}\mid x=a+b\sqrt{2},\ a,b \text{ 为有理数}\}$$

是 $\mathbf{R}$ 的一个子域.

事实上，若 $s\in S$，$s\neq 0$，设

$$s=a+b\sqrt{2},\quad a,b \text{ 为有理数}.$$

那么 $a-b\sqrt{2}\neq 0$，否则导致 $a=b\sqrt{2}$，或者 $b=0$ 且 $a=0$；或 $b\neq 0$，$a/b=\sqrt{2}$，两有理数之比为无理数，均引出矛盾. 于是

$$(a+b\sqrt{2})(a-b\sqrt{2})=a^2-2b^2\neq 0.$$

由于 a^2-2b^2 亦为有理数，所以

$$(a+b\sqrt{2})^{-1}=\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2}\in S.$$

据定义 2，S 是个域，它是实数域的一个子域.

例题 2　设 R 是个至少含两个元素的交换环. 那么，R 为域

的充分必要条件是，对任意 $a,b\in R$，$a\neq 0$，方程

$$ax=b$$

恒有唯一解，即有唯一确定的 $c\in R$ 使 $ac=b$.

证明　如果 R 是个域，任取方程

$$ax=b, \qquad (*)$$

只要 $a\neq 0$，则 a 必有乘法逆元 a^{-1}. 令 $c=a^{-1}b$，则

$$ac=a(a^{-1}b)=(aa^{-1})b=b;$$

也就是说 c 满足方程(*). 进一步，若还有 $d\in R$ 使 $ad=b$，那么，由

$$ad=b=ac, \quad a\neq 0$$

消去 a，立得 $d=c$. 这说明(*)的解是唯一的.

反之，若 R 中方程(*)当 $a\neq 0$ 时恒有唯一解. 由于它至少含两个元，可任取 $a\neq 0$，看方程

$$ax=a, \quad a\neq 0.$$

据假设，它有唯一解，设为 e. 可断言 e 为 R 的恒等元.

任取 $d\in R$. 设 $ad=b$，这意味着 d 是满足方程 $ax=b$ 的. 再由 e 满足 $ax=a$，即

$$ae=a$$

可得到

$$a(ed)=(ae)d=ad=b,$$

即 ed 也满足 $ax=b$. 据唯一性条件，必有

$$de=ed=d, \quad 对任意 d\in R,$$

这说明 e 为 R 的恒等元.

进一步，对任意 $d\in R$，$d\neq 0$，方程

$$dx=e$$

必有唯一解 f，即 $df=fd=e$. 从而 R 的每个非零元恒有逆元. R 是个域. ▮

命题 1　只含有限个元素的整环必为域.

证明　设 R 是个有限整环，那么 R 有 1 且可换，所以，据定

义 2 知,要证明 R 为域,只需验证它的每个非零元均有逆元即可.

任取 $a\in R$, $a\neq 0$,看元素

$$a, a^2, \cdots, a^n, \cdots.$$

由 R 的有限性,上述元素必出现重复.不妨设有正整数 k, l 使

$$a^k = a^l, \quad k < l.$$

又 $a^l = a^k \cdot a^{l-k}$,从而

$$a^k(1 - a^{l-k}) = 0. \tag{1}$$

而 a 不是零因子,进而 a^k 也不是零因子.于是,(1)式意味着 $1 - a^{l-k} = 0$,即

$$1 = a^{l-k} = a \cdot a^{l-k-1}, \quad l - k - 1 \geqslant 0.$$

这说明元素 a^{l-k-1}就是 a 的逆元素(注意,$l-k-1=0$ 时,$a^0 = 1$). ▎

例题 3 环 $\mathbf{I}_n$ 为域的充分必要条件是 n 为素数.

证明 若 n 不为素数,必有整数 p, q 使

$$n = pq, \quad 1 < p < n, \ 1 < q < n.$$

于是,在 $\mathbf{I}_n$ 中,$p^* \neq 0^*$, $q^* \neq 0$,但

$$p^* q^* = 0^*,$$

$\mathbf{I}_n$ 有非零的零因子.

反之,若 n 为素数,任取 $p^*, q^* \in \mathbf{I}_n$,当 p^* 和 q^* 均不为 0^* 时,必有

$$1 \leqslant p < n, \quad 1 \leqslant q < n.$$

由于 n 为素数,它不能整除 p,又不能整除 q,则必不能整除它们的乘积.设

$$pq = in + j, \quad 0 \leqslant j < n,$$

则 $j \neq 0$,也就是

$$p^* q^* = j^* \neq 0^*.$$

$\mathbf{I}_n$ 不含非零的零因子,且为有限环,由命题 1 知 $\mathbf{I}_n$ 必为域. ▎

下面讨论域的简单性质.

命题 2 域不含非平凡的理想.

证明 设 R 是个域, $I \neq \{0\}$ 是 R 的一个理想. 于是有 $a \in I$, $a \neq 0$. 但 R 是个域, a 在 R 中有逆元 a^{-1}, $a^{-1}a = 1$. 进而, 对任意 $r \in R$ 有

$$(ra^{-1})a \in I, \quad (I \text{ 是理想}),$$
$$r(a^{-1}a) \in I, \quad (\text{结合律}),$$
$$r \in I. \quad (a^{-1}a = 1).$$

故得 $R \subseteq I$, $R = I$. 也就是说 R 的理想除 $\{0\}$ 外只有 R 本身, 绝无其他. ▌

命题 3 设 φ 是环 R 到 S 的环同态, 且为满射. 如果 R 是个域, 则 φ 或者为同构映射, 或者将 R 所有元映成 S 的零元(φ 是零同态).

证明 看 φ 的核 $\mathrm{Ker}(\varphi)$, 它是环 R 的理想. 由命题 2 知 $\mathrm{Ker}(\varphi) = \{0\}$ 或 $\mathrm{Ker}(\varphi) = R$.

如果 $\mathrm{Ker}(\varphi) = R$, 即对任意 $r \in R$ 恒有 $\varphi(r) = 0$.

如果 $\mathrm{Ker}(\varphi) = \{0\}$, 在群论中多次遇到过, φ 必然是单射. 从而 φ 是同构映射. ▌

定义 3 域$(F, +, \cdot)$的子集 S 称为 F 的子域, 如果它是 F 的子环且它在 F 的运算之下本身是个域.

定义 4 设 R 是个环. 如果有自然数 m 使得, 对每个 $r \in R$ 均有 $mr = 0$, 而小于 m 的自然数都不具备该性质, 则说环 R 的**特征数**为 m. 如果找不到满足上述要求的自然数, 则说环 R 的特征数为 0.

我们来解释一下上面的定义, 看每个环是否都有一个特征数.

给定一个环 R. 那么, 或者有一个自然数 n 使得

$$na = 0, \quad \text{对每个 } a \in R. \qquad (*)$$

此时, 我们可以看具有上述性质的自然数的最小者 m. 它使得

$$ma = 0, \quad \text{对每个 } a \in R,$$

且当 $l < m$ 时(l 是自然数)必有 $b \in R$ 使得 $lb \neq 0$ (否则, l 亦具

(*)性质，与 m 之最小性矛盾)．于是知，m 即为 R 之特征数．

或者，任意自然数 k 都不具备(*)性质，于是，按定义，R 的特征数为 0．

这说明每个环都以一非负整数为其特征数．例如，整数环、有理数环、实的 $n\times n$ 矩阵环、实多项式环等特征数均为 0．而 $\mathbf{I}_n$ 的特征数为 n，因为对任意 $i^*\in\mathbf{I}_n$，都有 $n\cdot i^*=0^*$，而对任意 $m<n$，只要取 $1^*\in\mathbf{I}_n$ 即可看出 $m\cdot 1^*=m^*\neq 0^*$．

命题 4 有限环的特征数必整除其元数．

事实上，若 R 为 n 元环，$(R,+)$ 即为 n 元交换群．由拉格朗日定理，每个元素的加法周期均整除 n，即对任意 $a\in R$，$na=0$．由此可知，R 的特征数不为 0，设为 m．若 m 不能整除 n，则做除法得

$$n=qm+i,\quad 0<i<m,$$

那么，对任意 $a\in R$ 恒有

$$na=(qm)a+ia.$$

由于 $na=0$，$qma=0$，从而必有 $ia=0$．这与 a 的任意性、特征数 m 的最小性矛盾，故应有 m 能整除 n．▍

有限环之元素数与其特征数不相等的例子很多，如 $\mathbf{I}_2\oplus\mathbf{I}_2$ 之特征数为 2，元素数为 4．也并非只有有限环的特征数才能是有限的．

例 3 仿照第四章§1 之例 1．设 F 是实数域 $\mathbf{R}$ 到环 $\mathbf{I}_2$ 的所有映射的集合．规定，对任意 $f,g\in F$，

$$f\# g: x\to f(x)+g(x),\quad x\in\mathbf{R},$$

$$f\odot g: x\to f(x)g(x),\quad x\in\mathbf{R}.$$

则$(F,\#,\odot)$是个环，它有无穷多个元素，映射族

$$f_a(x)=\begin{cases}0^*, & 当\ x\neq a,\\ 1^*, & 当\ x=a\end{cases}$$

取不同的实数 a，就得到不同的映射，也就是 F 中不同的元素．

但是,环 F 的特征数为 2,因为对任意 $f \in F$,

$$(f \# f)(x) = f(x) + f(x) = 0^*, \quad x \in \mathbf{R}.$$

命题 5 域 F 的特征数或为 0 或为素数.

证明 设 F 的特征数为 m, m 不是素数,

$$m = pq, \quad 1 < p < m, 1 < q < m.$$

用 e 代表 F 的恒等元,应有

$$0 = me = (pq)e = (pe)(qe).$$

由于 F 是个域,不含零因子,故 $pe = 0$ 或 $qe = 0$.

如果 $pe = 0$,那么,对任意 $a \in F$,有

$$\begin{aligned} pa &= p(ea) && (e \text{ 是恒等元}) \\ &= (pe)a && (\text{分配律}) \\ &= 0. && (pe = 0) \end{aligned}$$

这与 m 是特征数的极小性矛盾.

当 $qe = 0$ 时,也是一样. ▌

命题 6 设域 F 的特征数为 $p \neq 0$. 那么,对任意 $a, b \in F$,恒有 $(a+b)^p = a^p + b^p$.

分析 在一般非交换环中,我们不能随便将 $(a+b)^2$ 写成 $a^2 + 2ab + b^2$. 因为,按分配律算

$$(a+b)^2 = a^2 + ab + ba + b^2,$$

ab 可能不等于 ba.

当 R 为交换环时,可用归纳法证明二项式公式

$$(a+b)^n = a^n + na^{n-1}b + \cdots + nab^{n-1} + b^n.$$

证明 因为

$$(a+b)^p = a^p + pa^{p-1}b + p(p-1)a^{p-2}b^2 + \cdots + b^p,$$

上式右端除首末两项外均为某元之 p 倍,而 p 为 F 的特征数,它们必为 0,所以 $(a+b)^p = a^p + b^p$. ▌

本节最后,我们用抽象代数方法处理一个数论问题,论证十分简洁.

例题 4(Fermat 小定理) 设 p 是个素数. 如果整数 a 不能被

p 整除，则 p 必整除 $a^{p-1}-1$.

证明 由于 p 是素数，故

$$\mathbf{I}_p \cong \mathbf{I}/(p) = \mathbf{I}_{-p}$$

为域. a 不能被 p 整除，$a \notin (p)$，从而 a 在 $\mathbf{I}$ 对 (p) 的等价类

$$[a] \neq [0] = (p).$$

又因为 $\mathbf{I}/(p)$ 是个域，它的所有非零元素构成一个乘法群，是个 $p-1$ 阶群. 故

$$[a]^{p-1} = [1].$$

注意 $\mathbf{I}/(p)$ 中乘法的定义，即知

$$[a]^{p-1} = [a^{p-1}] = [1],$$

从而 $a^{p-1} \in [1]$，p 整除 $a^{p-1}-1$. ∎

命题 7 设环 $(R,+,\cdot)$ 有 1. 那么，当 1 在群 $(R,+)$ 中阶数无限时，R 之特征数为 0；当 1 的阶数为正整数 n 时，R 之特征数恰为 n.

证明 若 1 在 $(R,+)$ 不是有限阶的，那么，对任意正整数 m，恒有 $m\cdot 1 \neq 0$，从而 R 的特征数为 0.

若 1 在 $(R,+)$ 中阶数为 n，n 为正整数，那么，对任意 $a \in R$，必有

$$na = n(1a) = (n\cdot 1)a = 0,$$

且 $(n-1)\cdot 1 \neq 0$. 故 R 之特征数为 n. ∎

例题 5 用 $(\mathbf{Q},+)$ 代表有理数加法群，用 $(\mathbf{I},+)$ 代表整数加法群，用 $(M,+)$ 表示 $(\mathbf{Q},+)$ 对 $(\mathbf{I},+)$ 的商群. 那么，不管用什么方法定义 M 上乘法 $\times$ 使得 $(M,+,\times)$ 成环，该环都不会有恒等元.

证明 设 $(M,+,\times)$ 是个环. M 中的每个元素就是 $(\mathbf{I},+)$ 在 $(\mathbf{Q},+)$ 中的一个陪集，必形如

$$\frac{a}{b} + \mathbf{I}, \quad a, b \in \mathbf{I},\ b \neq 0.$$

进一步，还可以要求 b 是个正整数．那么将该元自己加自己，加 b 次，得

$$\left(\frac{a}{b}+\cdots+\frac{a}{b}\right)+\mathbf{I}=a+\mathbf{I}=\mathbf{I},$$

$\mathbf{I}$ 实际上是 M 中的零元素．从而说明，M 中每个元素的阶数都有限．

假设环 $(M,+,\times)$ 有恒等元 $\bar{e}$，

$$\bar{e}=\frac{a}{b}+\mathbf{I},\quad a,b\in\mathbf{I},\ b>0.$$

那么，b 个 $\bar{e}$ 相加得 $b\bar{e}=\mathbf{I}$，$\bar{e}$ 在 $(M,+)$ 中阶数有限．据命题 7 知，环 M 的特征数为 k，k 是个正整数．

但是，看 M 中元素 $\frac{k}{k+1}+\mathbf{I}$，则有

$$k\left(\frac{k}{k+1}+\mathbf{I}\right)=\frac{k^2}{k+1}+\mathbf{I}=\left(\frac{k^2-1}{k+1}+\mathbf{I}\right)+\left(\frac{1}{k+1}+\mathbf{I}\right),$$

由于

$$\frac{k^2-1}{k+1}=k-1,\quad (k-1)+\mathbf{I}=\mathbf{I},$$

知

$$k\left(\frac{k}{k+1}+\mathbf{I}\right)=\frac{1}{k+1}+\mathbf{I}\neq\mathbf{I},$$

矛盾．$(M,+,\times)$ 不能有乘法恒等元． ▌

习 题 一

1．设 R 是个交换环，$a,b\in R$．若 $ab\neq0$，ab 也不是零因子，那么 $a\neq0$，a 也不是零因子．

2．设 F 和 F' 是域，σ 是从 F 到 F' 的非零的环同态映射．用 1 和 $1'$ 表示 F 和 F' 的恒等元，则必有 $\sigma(1)=1'$．当 F 和 F' 是一般环时，此事对吗？

3．设 D 是个整环，$a,b,c\in D$．若有 $d\in D$ 使得

$$d^3-(a+b+c)d^2+(ab+bc+ca)d-abc=0,$$

则 d 必为 a,b,c 中的一个.

4. 证明:所有的三元域都是同构的.

5. 设域 F 含 m 个元素. 证明:对任意 $a\in F$, $a\neq 0$, 必有 $a^{m-1}=1$. 对任意 $a\in F$, 必有 $a^m=a$.

6. 在复数环 C 中,

$$R=\{a+b\sqrt{-7}\mid a,b\text{ 是实数}\}$$

是个子环, R 本身是个除环.

§2 理想与商环(Ⅱ)

在§1,我们看到,域的同态像或为$\{0\}$或为域. 现在,反过来问,什么环的同态像能够是个域呢?

例1 用 $\mathbf{P}$ 代表所有实系数多项式所构成的环. 来建立一个 $\mathbf{P}$ 到复数域 $\mathbf{C}$ 的映射.

任取 $f(x)\in\mathbf{P}$,用多项式 x^2+1 去除,得

$$f(x)=q(x)(x^2+1)+\alpha x+\beta,$$

其中余式 $\alpha x+\beta$ 是由 $f(x)$ 完全确定的. 令

$$\varphi: f(x)\to\alpha\mathrm{i}+\beta,\quad \mathrm{i}=\sqrt{-1},$$

就得到 $\mathbf{P}$ 到 $\mathbf{C}$ 的一个映射.

任取 $f(x),g(x)\in\mathbf{P}$,设

$$f(x)=q(x)(x^2+1)+\alpha x+\beta,$$
$$g(x)=p(x)(x^2+1)+\gamma x+\delta.$$

那么,有

$$f(x)+g(x)=[q(x)+p(x)](x^2+1)+(\alpha+\gamma)x+\beta+\delta,$$
$$f(x)g(x)=k(x)(x^2+1)+\alpha\gamma x^2+(\alpha\delta+\beta\gamma)x+\beta\delta,$$
$$=l(x)(x^2+1)+(\alpha\delta+\beta\gamma)x+(\beta\delta-\alpha\gamma).$$

所以,

$$\varphi[f(x)+g(x)]$$
$$=(\alpha+\gamma)\mathrm{i}+(\beta+\delta)\qquad(\varphi\text{ 的定义})$$

$$= (\alpha i + \beta) + (\gamma i + \delta) \qquad \text{(复数加法)}$$
$$= \varphi[f(x)] + \varphi[g(x)]. \qquad (\varphi\ \text{的定义})$$

而且

$$\varphi[f(x)g(x)]$$
$$= (\alpha\delta + \beta\gamma)i + (\beta\delta - \alpha\gamma) \qquad (\varphi\ \text{的定义})$$
$$= (\alpha i + \beta)(\gamma i + \delta) \qquad \text{(复数乘法)}$$
$$= \varphi[f(x)]\varphi[g(x)]. \qquad (\varphi\ \text{的定义})$$

这说明 φ 是 $\mathbf{P}$ 到 $\mathbf{C}$ 的环同态映射.

任取 $\alpha i + \beta \in \mathbf{C}$,则

$$\varphi[\alpha x + \beta] = \alpha i + \beta,$$

故 φ 为满同态.

计算

$$\mathrm{Ker}(\varphi) = \{f(x) \in \mathbf{P} \mid \varphi f[(x)] = 0\}.$$

显然,$f(x) \in \mathrm{Ker}(\varphi)$之充要条件是 x^2+1 整除 $f(x)$,充分必要条件是 $f(x)$属于 x^2+1 在 $\mathbf{P}$ 中生成的理想(x^2+1). 即

$$\mathrm{Ker}(\varphi) = (x^2+1).$$

由环同态基本定理,知 $\mathbf{P}/(x^2+1) \cong \mathbf{C}$. ▌

环的同态像的性质由该环及一个理想(同态核)决定. 上例说明,$\mathbf{P}$ 对理想(x^2+1)的剩余环为域,那么,$\mathbf{P}$ 有无真理想(即非平凡理想)A 使剩余环 $\mathbf{P}/A$ 不是域呢?

例 2 在实多项式环 $\mathbf{P}$ 中,用 A 代表多项式 x^2-1 生成的理想(x^2-1), $\overline{f(x)}$代表多项式 $f(x)$所在的陪集 $f(x)+A$.

因为 $x-1 \notin A$,故$\overline{x-1} \neq \overline{0} = A$. 同样$\overline{x+1} \neq \overline{0}$. 但是,$(x+1)(x-1) = x^2-1 \in A$,故

$$\overline{x-1} \cdot \overline{x+1} = \overline{(x+1)(x-1)} = \overline{0}.$$

这说明环 $\mathbf{P}/A$ 有非零的零因子,当然环 $\mathbf{P}/A$ 不是个域.

定义 1 环 R 的理想 $M \neq R$ 称之为 R 的一个**极大理想**,如果对 R 的任意理想 A, $M \subseteq A$ 且 $M \neq A$ 蕴涵 $A = R$.

换言之,在 R 中真比 A 大的理想只有环 R 本身.

读者绝不可以将“A 是 R 的极大理想”理解为“A 是 R 的最大的真理想，它包含 R 的所有真理想”. 因为，假如用理想包含关系意味其大小的话，可能有些理想是不能比较谁大谁小的.

例 3 环 $\mathbf{I}_{12}$ 中，理想

$$A=\{0^*,3^*,6^*,9^*\},$$

$$B=\{0^*,2^*,4^*,6^*,8^*,10^*\}$$

都有极大理想. 因为，如果有 $\mathbf{I}_{12}$ 的理想 $M\neq A$ 且 $A\subseteq M$，M 有 t 个元素，那么，作为有限群，由拉格朗日定理，必有 4 整除 t，t 整除 12，且 $t\neq 4$. 故 $t=12$，$M=\mathbf{I}_{12}$. A 是极大理想. 同理可说明 B 也是 $\mathbf{I}_{12}$ 的一个极大理想.

当环为单环时，它不含非零真理想，真包含零理想者只有环本身. 故零理想是它的一个极大理想，而且只有这一个极大理想.

例题 1* 所有形如

$$\begin{pmatrix}0 & \frac{m}{n}\\ 0 & 0\end{pmatrix},\quad m,\ n\in\mathbf{I},\ n>0$$

的矩阵作成 $\mathbf{Q}$ 上 2 阶全阵环的一个子环，记为 R. 证明：R 没有极大理想.

证明 设 J 是 R 的一个非零理想且 $J\neq R$. 那么，必有整数 s,t 和 k，l 使得 $t\neq 0$，$l\neq 0$ 且

$$Q_{2\times 2}\neq\begin{pmatrix}0 & \frac{s}{t}\\ 0 & 0\end{pmatrix}\in J,\quad \begin{pmatrix}0 & \frac{k}{l}\\ 0 & 0\end{pmatrix}\notin J. \qquad (*)$$

由于 J 对减法封闭，左侧矩阵之 t 倍亦必在 J 中，即

$$\sigma=\begin{pmatrix}0 & s\\ 0 & 0\end{pmatrix}\in J,\quad \text{不妨设 } s>0.$$

同样由 J 的减法封闭性，知矩阵

$$\rho=\begin{pmatrix}0 & \frac{1}{l}\\ 0 & 0\end{pmatrix}\notin J.$$

否则，(*)右端的矩阵就在 J 中了.

由于 R 中任意两矩阵之积恒为零矩阵，由元素 ρ 生成的理想 (ρ) 表达起来非常简单，

$$(\rho)=\{m\rho \mid m\in \mathbf{I}\}.$$

因为 $\rho\notin J$，所以 $J+(\rho)\neq J$.

现断言，$J+(\rho)\neq R$. 我们可以证明，矩阵

$$\tau=\begin{pmatrix}0 & \frac{1}{sl^2}\\ 0 & 0\end{pmatrix}\notin J+(\rho).$$

若不然，$\tau\in J+(\rho)$，则必有 $x\in J$，$m\in\mathbf{I}$ 使

$$\tau=x+m\rho. \qquad (*)$$

由于 J 是理想，对加减法封闭，看 sl 个 τ 之和，则有

$$sl\tau=\begin{pmatrix}0 & \frac{1}{l}\\ 0 & 0\end{pmatrix}=\rho.$$

然而，注意(*)，又有 $sl\tau=slx+slm\rho$. 由于 J 是个理想，故

$$slx\in J.$$

同时，又因为

$$msl\rho=msl\begin{pmatrix}0 & \frac{1}{l}\\ 0 & 0\end{pmatrix}=m\begin{pmatrix}0 & s\\ 0 & 0\end{pmatrix}=m\sigma,$$

而且 $\sigma\in J$，知道 $msl\rho=m\sigma\in J$.

从而 $\rho=sl\tau=slx+slm\rho\in J$，矛盾.

因为已经知道 R 有非零理想，且对 R 的任意非零理想 J，$J\neq R$，都能造出 R 的理想 $J+(\rho)$ 使得

$$J\neq J+(\rho)\neq R;$$

也就是说，R 的每个理想 $J\neq R$ 都不是 R 的极大理想. ▌

定理 1 设 R 是个有 1 的交换环，A 是它的一个理想. 那么，剩余环 R/A 为域的充分必要条件是 A 为 R 的一个极大理想.

证明 设 A 是 R 的一个极大理想. 因为恒等元 $1\notin A$(否则

推出 R 中任意元 $a=a\cdot 1\in A$)，故 R/A 中陪集 $1+A$ 不等于陪集 A，R/A 至少含两个元素且 $1+A$ 是 R/A 的恒等元.

可以断言，R/A 中的任意非零元 $a+A$(也就是 $a\notin A$)在 R/A 中必然有逆. 也就是，必能在 R/A 中找一元素 $b+A$ 使

$$(a+A)(b+A)=ab+A=1+A.$$

此事又等于要找一个 $b\in R$ 使得 $1\in ab+A$.

由于 R 是有 1 的交换环，元素 a 生成的理想

$$(a)=\{y\in R\mid y=ax\}.$$

由于 $(a)+A$ 也是 R 的理想，且 $a\notin A$，故

$$A\subseteq(a)+A,\quad A\neq(a)+A.$$

由 A 的极大性，推知 $(a)+A=R$.

于是，$1\in(a)+A$，有 $b\in R$，使得

$$1\in ab+A,\quad 1+A=(a+A)(b+A).$$

$b+A$ 就是 $a+A$ 的逆.

R/A 是个域.

反过来，设 R/A 是个域，来证明 A 为 R 的一个极大理想.

设 B 是 R 的理想，$A\subseteq B$，$A\neq B$. 那么，必有 $b\in B$，$b\notin A$，$b+A\neq A$，$b+A$ 是环 R/A 的非零元. 由于 R/A 是个域，$b+A$ 在 R/A 中有逆元，即必有 $c\in R$ 使

$$(b+A)(c+A)=1+A,\quad 1=bc+a,\ a\in A.$$

但是，$b\in B$，B 是理想，故 $bc\in B$. 再加上 $a\in A\subseteq B$，即得到 $1\in B$，从而 R 的任意元都属于 B，$R=B$.

这说明，A 为 R 的一个极大理想. ▮

与此问题类似，设 A 为环 R 的理想，何时剩余环 R/A 为无零因子环、为有 1 环、为交换环，等等.

定义 2 设 R 是个交换环，P 是 R 的一个理想. 如果，$P\neq R$ 且对任意 $a,b\in R$，$ab\in P$ 蕴涵，$a\in P$ 或 $b\in P$，则说 P 是 R 的一个**素理想**. 如果 $\{0\}$ 是环 R 的素理想，则说 R 是个**素环**.

例如，环 R 是个交换的无零因子环，那么，它的零理想 $\{0\}$ 是

它的一个素理想.

又如,整数环 I 中,素数 p 生成的主理想 (p) 必为 I 的素理想.因为,若 $m,n\in I$ 使 $mn\in(p)$,即 mn 是 p 的整数倍,p 整除 mn.但 p 是素数,整除两整数之积时必整除两因子之一.p 整除 m 时,$m\in(p)$;p 整除 n 时,$n\in(p)$.

命题 1 设 R 是个交换环.那么,环 R 的理想 $P(\neq R)$ 为其素理想的充分必要条件是剩余环 R/P 为无零因子环.

证明 如果环 R/P 为无零因子环,又有 $a,b\in R$ 使得 $ab\in P$.那么,有

$$(a+P)(b+P)=ab+P=P.$$

因为 R/P 不含非零之零因子,它的两个元素,$a+P$ 和 $b+P$ 之积为零元,必至少有一个是零元,即 $a+P=P$ 或 $b+P=P$,此事等价于

$$a\in P \text{ 或 } b\in P,$$

故 P 为素理想.

反之,设 P 是 R 的一个素理想,在 R/P 中有元素 $a+P$ 和 $b+P$ 之积为零,即

$$(a+P)(b+P)=ab+P=P.$$

也就是 $ab\in P$.由于 p 是素理想,这就意味着

$$a\in P \text{ 或 } b\in P$$

即 $a+P=P$ 或 $b+P=P$, R/P 为无零因子环. ∎

命题 2 设 R 是个环,A 是 R 的理想.环 R/A 为交换环的充分必要条件是 A 包含 R 中所有形如

$$xy-yx,\quad x,y\in R$$

的元素.

证明 设 R/A 是个交换环.任取 $x,y\in R$ 就得到 R/A 的两个元素 $x+A$ 和 $y+A$.由于 R/A 是个交换环,必有

$$\begin{aligned}&(x+A)(y+A)\\&\quad=xy+A \qquad\qquad (R/A\text{ 中乘法})\end{aligned}$$

$$= (y+A)(x+A) \qquad (R/A \text{ 是交换环})$$
$$= yx + A \qquad (R/A \text{ 中乘法})$$
也就是 $xy + A = yx + A$，$xy - yx \in A$.

反之，设理想 A 包含所有形如 $xy - yx$，$x, y \in R$ 的元素. 那么，任取 R/A 的元素 $a + A$，$b + A$，由于 $ab - ba \in A$，$ab + A = ba + A$，就有
$$(a+A)(b+A) = ab + A = ba + A = (b+A)(a+A).$$
从而证明了 R/A 为交换环. ▌

例题 2 设 R 是个交换环. 对任意 $a \in R$，证明：
$$N_a = \{x \in R \mid x = ar - r,\ r \in R\}$$
是 R 的理想，且 R 的理想 $A \neq R$ 使 R/A 有恒等元的充分必要条件是有 $b \in R$，$N_b \subseteq A$.

证明 任取 $x, y \in N_a$，$z \in R$，
$$x = ar - r,\ y = as - s,\ r, s \in R$$
则 $x - y = a(r-s) - (r-s) \in N_a$，且
$$xz = (ar - r)z = a(rz) - rz \in N_a,$$
因为 R 为交换环同样可证
$$zy = z(as - s) = a(zs) - zs \in N_a$$
故集合 N_a 是 R 的理想.

如果，有 $b \in R$，$N_b \subseteq A$，即对任意 $r \in R$，
$$br - r \in A,$$
也就是 $br + A = r + A$. 从而
$$(b+A)(r+A) = r + A, \quad r \in R.$$
因为 R 为交换环同样可证
$$(r+A)(b+A) = r + A, \quad r \in R$$
这说明 $b + A$ 是 R/A 的恒等元.

反之，假设 R/A 有恒等元 $b + A$. 那么，对任意 $r \in R$，$r + A \in R/A$，有

$$(b+A)(r+A)=br+A=r+A$$

也就是 $br-r\in A$, $N_b\subseteq A$. ▌

当环 R 有恒等元 1 时,$N_1=\{0\}$,它含在每个理想里,故 R 的每个商环都是有恒等元的.这一点,在讨论环的同态像时,已经说过了.

例题 3 设 R 是个有 1 的交换环. R 的元素 a 称为是幂零的,如果有正整数 n 使 $a^n=0$. 证明:R 的所有幂零元的集合 N 是 R 的一个理想.而且商环 R/N 中没有非零幂零元.

分析 元素幂零时,正整数 n 的选择可能随元素 a 不同而变化.例如,在实的 3 阶矩阵环 $M_{3\times 3}$ 中,矩阵

$$\begin{pmatrix}0&0&0\\0&0&0\\0&0&0\end{pmatrix},\quad \begin{pmatrix}0&0&0\\0&0&0\\1&0&0\end{pmatrix},\quad \begin{pmatrix}0&0&0\\1&0&0\\0&1&0\end{pmatrix}$$

都是幂零的,分别选取 $n=1,2,3$ 即可.当然,对这 3 个矩阵都取 $n=3$ 也行.但是,在任意环中给出无穷多个幂零元,要找出一个正整数 n 使每个幂零元的 n 次方都等于 0,并不是一定能办到的.

证明 任取 $a,b\in N$. 据 N 的定义,必有正整数 m,n 使 $a^m=0$, $b^n=0$. 但是,

$$\begin{aligned}(a-b)^{m+n}=a^{m+n}+(m+n)a^{m+n-1}b+\cdots\\+(m+n)ab^{m+n-1}+b^{m+n}.\end{aligned}$$

等式右端每加项中,或者 a 的方次超过 m 或者 b 的方次超过 n,从而每个加项均为 0,即

$$(a-b)^{m+n}=0,$$

据 N 的定义,$a-b\in N$.

任取 $a\in N$, $r\in R$. 设 $a^m=0$,那么

$$(ra)^m=r^m a^m=0,$$

从而知道 $ra\in N$.

所以,N 是 R 的理想.

进一步,设 $a+N$ 是 R/N 的一个幂零元,设有正整数 m 使

$$(a+N)^m=N.$$

由 R/N 乘法定义，可得 $a^m\in N$. 这说明 a^m 是环 R 的一个幂零元，对于这个 a^m 又必有 n 使得

$$(a^m)^n=a^{mn}=0.$$

从而 $a\in N$. $a+N$ 就是 R/N 的零元. 即，商环 R/N 不含非零幂零元. ▎

想得到环的具有某种性质的同态像，往往可以把环对环中那些破坏此性质的元素生成的理想作商环来得到. 这种方法在抽象代数学中很有用.

习 题 二

1. 设 p 是个素数. 给出商环 $\mathbf{I}/(p^2)$ 的所有极大理想.

2. 设 D 是个整环，I 是 D 的理想，$I\neq D$. 证明：I 为 D 的素理想的充分必要条件是 D 的子集 $D-I$ 在 D 的乘法之下封闭.

3. 设环 R 有 1，R 的理想 $M\neq R$，且 $R-M$ 的每个元都是 R 的单位. 证明：M 是 R 的一个极大理想.

4*. 设 f 是环 R 到环 R' 的满的同态映射. 证明：若 P 是 R 的素理想且 $\mathrm{Ker}(f)\subseteq P$，则 $f(P)$ 是 R' 的素理想；若 P' 是 R' 的素理想，则 $f^{-1}(P')$ 是 R 的素理想.

5. 设 R 是个交换的素环，且对每个元素 $a\in R$ 恒有一个由 a 决定的整数 $n>1$ 使得 $a^n=a$. 证明：R 必为除环.

§3 嵌 入 问 题

环如果有恒等元，那么，其主理想的元素表达起来相当简洁，且该环必有极大理想，等等. 这些性质给深入讨论环的结构带来极大方便.

环如果是个域，它的乘法就有了一个“逆运算”，这使得很多在一般环中无从下手的问题在域中可以顺利解决，例如解各种形式的“方程式”.

给定一个环，它可能没有恒等元，更可能不是域. 那么，这个环

能不能看成是某个有恒等元环的子环，特别是某个域的子环呢？这就是我们要讨论的嵌入问题.

假如，环 R 可以嵌入一个环 K，即环 R 可以视为 K 的子环，那么，研究 R 时就可以利用环 K 的性质，K 可能有恒等元，可能为域.

命题 1 设 R 是个环，$\mathbf{I}$ 是整数环. 在集合 $\mathbf{I}\times R$ 中，规定运算，对任意 $(m,a),(n,b)\in \mathbf{I}\times R$，

$$(m,a)\#(n,b)=(m+n,a+b),$$
$$(m,a)\odot(n,b)=(mn,mb+na+ab).$$

则 $(\mathbf{I}\times R,\#,\odot)$ 是个环，R 同构于它的一个子环.

证明 对于运算 #，我们用 θ 代表环 R 的零元素时，容易看出，对任意 $(m,a)\in \mathbf{I}\times R$，有

$$(m,a)\#(0,\theta)=(m,a).$$

对任意 $(m,a)\in \mathbf{I}\times R$，元素 $(-m,-a)\in I\times R$ 使

$$(m,a)\#(-m,-a)=(0,\theta).$$

同时，运算 # 满足交换律和结合律.

$(\mathbf{I}\times R,\#)$ 是个交换群.

对于运算 $\odot$，任取 $(m,a),(n,b),(k,c)\in \mathbf{I}\times R$ 都有

$$\begin{aligned}
&[(m,a)\odot(n,b)]\odot(k,c)\\
&\quad=(mn,mb+na+ab)\odot(k,c)\\
&\quad=(mnk,kmb+kna+kab+mnc+mbc+nac+abc)\\
&\quad=(m,a)\odot(nk,kb+nc+bc)\\
&\quad=(m,a)\odot[(n,b)\odot(k,c)],
\end{aligned}$$

即 $\odot$ 满足结合律.

分配律的验证也只是些极简单的演算. 所以，$(\mathbf{I}\times R,\#,\odot)$ 是个环，且 $(1,\theta)$ 是恒等元.

现在，令 $\varphi: a\to(0,a)$. 则 φ 是环 R 到 $\mathbf{I}\times R$ 的一个映射，还是个环的同态映射. 记 $\mathbf{I}\times R$ 的子环

$$\bar{R}=\mathrm{Img}(\varphi)=\{(m,a)\in \mathbf{I}\times R \mid m=0\},$$

由于 φ 是单射，故 φ 是 R 到 $\bar{R}$ 的同构映射.

也就是说，环($\mathbf{I}\times R$，#，⊙)含一子环 $\bar{R}$，$\bar{R}$ 同构于 R. ▌

注意，当 R 本身有恒等元 e 时，上述嵌入仍可照样进行，一般来说 $(0,e)$ 不是($\mathbf{I}\times R$，#，⊙)的恒等元.

推论 任意交换环 R 必同构于一个有 1 的交换环的子环. ▌

命题 2 特征数为 n 的环恒同构于一个特征数为 n 的有 1 环的子环.

证明 当 $n=0$ 时，命题 1 中所构造的环($\mathbf{I}\times R$，#，⊙)的特征数也是 0.

当环 R 特征数 $n\neq 0$ 时，仿上命题 1 的证明，在集合 $\mathbf{I}_n\times R$ 上定义

$$(i^*,a)\#(j^*,b)=(i^*+j^*,a+b),$$
$$(i^*,a)\odot(j^*,b)=(i^*\cdot j^*,ib+ja+ab).$$

则($\mathbf{I}_n\times R$，#，⊙)也构成环.

在验证各种条件时，只要注意 R 特征数为 n，则对任意 $a\in R$ 都有 $na=0$.

元素 $(1^*,0)$ 是($\mathbf{I}_n\times R$，#，⊙)的恒等元. 该环之特征数亦为 n.

环 R 同构于($\mathbf{I}_n\times R$，#，⊙)的子环.

$$\bar{R}=\{(i^*,a)\in\mathbf{I}_n\times R\mid i^*=0^*\}.$$ ▌

定理 1 设 R 是个交换的无零因子环. 那么，R 必同构于某个域的一个子环.

证明 当 R 只含一个元素即零元时，R 可视为任何域的子环 $\{0\}$ 的同构像.

以下不妨设 R 至少含两个元素，用英文字母 $a,b,c,\cdots$ 表示它的元素. R_0 代表 R 之所有非零元的集合，R_0 当然不是空集.

下面我们做一个域来满足定理的各项要求.

第一步 在集合 $R\times R_0$ 上定义一个关系，说 $(a,b)\sim$

(a',b'),如果 $ab'=a'b$.这是一个等价关系.因为

(1) 对任意$(a,b)\in R\times R_0$,由 $ab=ab$ 知

$$(a,b)\sim(a,b),$$

(2) 如果$(a,b)\sim(a',b')$,则 $ab'=a'b$,故又得

$$(a',b')\sim(a,b),$$

(3) 如果$(a,b)\sim(c,d)$且$(c,d)\sim(e,f)$即

$$ad=cb,cf=ed,$$

于是,$afd=adf=cbf=bcf=bed=ebd$,但 R 无非零的零因子,消去律成立,即得到 $af=eb$(因 $d\neq0$).故$(a,b)\sim(e,f)$.

第二步 用等价关系$\sim$将集合 $R\times R_0$ 分成等价类.用

$$\left\{\frac{a}{b}\right\}$$

代表元素(a,b)所在的等价类.$R\times R_0$ 在等价关系$\sim$之下的商集,记为 Q,即

$$Q=\left\{\left\{\frac{a}{b}\right\},\left\{\frac{c}{d}\right\},\cdots\right\}.$$

第三步 在 Q 上定义运算$\#$,对任意

$$\left\{\frac{a}{b}\right\},\left\{\frac{c}{d}\right\}\in Q$$

规定

$$\left\{\frac{a}{b}\right\}\#\left\{\frac{c}{d}\right\}=\left\{\frac{ad+cb}{bd}\right\}.$$

首先,因为 $b,d\in R_0$, b,d 不为 0,R 不含非零零因子,故 $bd\neq0$, $(ad+cb,bd)\in R\times R_0$.从而

$$\left\{\frac{ad+cb}{bd}\right\}$$

是 Q 中确定元素.

其次,应当注意,上面规定,表面上与等价类的代表元素选择有关系,涉及到定义的合理性问题.设

$$\left\{\frac{a}{b}\right\}=\left\{\frac{a'}{b'}\right\},\quad \left\{\frac{c}{d}\right\}=\left\{\frac{c'}{d'}\right\},$$

那么,有 $ab'=a'b$ 和 $cd'=c'd$.从而

$$ab'dd'=a'bdd',\quad cd'bb'=c'dbb',$$
$$(ad+bc)b'd'=(a'd'+b'c')bd;$$

也就是$(ad+bc,bd)\sim(a'd'+b'c',b'd')$,即

$$\left\{\frac{ad+bc}{bd}\right\}=\left\{\frac{a'd'+b'c'}{b'd'}\right\}.$$

运算#的定义是合理的,称#为 Q 上的加法.

第四步 验证$(Q,\#)$是个交换群.

(1) 任取 $a,b,c\in R$, $b,d,f\in R_0$ 都有,

$$\left\{\frac{a}{b}\right\}\#\left(\left\{\frac{c}{b}\right\}\#\left\{\frac{e}{f}\right\}\right)=\left\{\frac{a}{b}\right\}\#\left\{\frac{cf+de}{df}\right\}$$
$$=\left\{\frac{adf+bcf+bde}{bdf}\right\},$$
$$\left(\left\{\frac{a}{b}\right\}\#\left\{\frac{c}{d}\right\}\right)\#\left\{\frac{e}{f}\right\}=\left\{\frac{ad+bc}{bd}\right\}\#\left\{\frac{e}{f}\right\}$$
$$=\left\{\frac{adf+bcf+bde}{bdf}\right\},$$

即满足结合律.交换律是显然成立的.

(2) 取 $b\in R_0$,则

$$\left\{\frac{0}{b}\right\}\#\left\{\frac{c}{d}\right\}=\left\{\frac{c}{d}\right\}\#\left\{\frac{0}{b}\right\}=\left\{\frac{bc}{bd}\right\}=\left\{\frac{c}{d}\right\},$$

即 Q 有加法零元.可用任意$(0,b)$代表之,记为 $0_\#$.

(3) 对任意 $a\in R$, $b\in R_0$,有

$$\left\{\frac{a}{b}\right\}\#\left\{\frac{-a}{b}\right\}=\left\{\frac{0}{bb}\right\}=0_\#.$$

所以,$(Q,\#)$是个交换群.

第五步 在 Q 上定义运算$\odot$,对任意

$$\left\{\frac{a}{b}\right\},\left\{\frac{c}{d}\right\}\in Q$$

规定

$$\left\{\frac{a}{b}\right\}\odot\left\{\frac{c}{d}\right\}=\left\{\frac{ac}{bd}\right\}.$$

首先,$bd\neq0$, (ac,bd)有意义.

其次,若

$$\left\{\frac{a}{b}\right\}=\left\{\frac{a'}{b'}\right\},\quad \left\{\frac{c}{d}\right\}=\left\{\frac{c'}{d'}\right\},$$

则由 $ab'=a'b$, $cd'=c'd$ 推出$acb'd'=a'c'bd$.从而

$$\left\{\frac{ac}{bd}\right\}=\left\{\frac{a'c'}{b'd'}\right\},$$

即定义是合理的.称$\odot$为 Q 上乘法.

第六步 $(Q,\#,\odot)$是个环.

(1) Q 的乘法满足结合律和交换律.

(2) 对任意 $a,c,e\in R$, $b,d,f\in R_0$,有

$$\left\{\frac{a}{b}\right\}\odot\left(\left\{\frac{c}{d}\right\}\#\left\{\frac{e}{f}\right\}\right)=\left\{\frac{a}{b}\right\}\odot\left\{\frac{cf+de}{df}\right\}=\left\{\frac{acf+ade}{bdf}\right\},$$

$$\left(\left\{\frac{a}{b}\right\}\odot\left\{\frac{c}{d}\right\}\right)\#\left(\left\{\frac{a}{b}\right\}\odot\left\{\frac{e}{f}\right\}\right)=\left\{\frac{ac}{bd}\right\}\#\left\{\frac{ae}{bf}\right\}$$

$$=\left\{\frac{b(caf+ade)}{b(bdf)}\right\}.$$

由于 $b\neq0$,可推出上两式之右端相等.Q 满足分配律.

第七步 $(Q,\#,\odot)$是个域.

(1) 任取 $d,d\in R_0$, $bd=db$,即

$$(b,b)\sim(d,d),\quad \left\{\frac{b}{b}\right\}=\left\{\frac{d}{d}\right\}.$$

而且,对任意 $e\in R$, $f\in R_0$ 有

$$\left\{\frac{e}{f}\right\}\odot\left\{\frac{b}{b}\right\}=\left\{\frac{be}{bf}\right\}=\left\{\frac{e}{f}\right\}.$$

R 有恒等元,可用任意(b,b)作代表,记为 $1_{\odot}$.

(2) 我们在讨论加法时已经知道,任取元素 $b\neq0$, $(0,b)$所在等价类

$$\left\{\frac{0}{b}\right\}$$

就是 Q 的零元.任取 Q 的非零元

$$\left\{\frac{e}{f}\right\} \neq \left\{\frac{0}{b}\right\},$$

必有 $e \neq 0$.从而有

$$\left\{\frac{e}{f}\right\} \odot \left\{\frac{f}{e}\right\} = \left\{\frac{ef}{ef}\right\} = 1_{\odot},$$

即每个非零元均有逆.

第八步 建立一个从 R 到 Q 的单的环同态映射.

首先,取定 $r \in R$,那么,对任意 $b, d \in R_0$ 都有 $(rb)d = (rd)b$,也就是

$$\left\{\frac{rb}{b}\right\} = \left\{\frac{rd}{d}\right\}.$$

令

$$\varphi: r \rightarrow \left\{\frac{rb}{b}\right\}, \quad \text{任取 } b \in R_0$$

得到 R 到 Q 的一个映射.

其次,对任意 $r, s \in R$,有

$$\begin{aligned}
\varphi(rs) &= \left\{\frac{rsb}{b}\right\} && (\varphi \text{ 的定义}) \\
&= \left\{\frac{rbsb}{bb}\right\} && (b \neq 0, \text{取不同代表元}) \\
&= \left\{\frac{rb}{b}\right\} \odot \left\{\frac{sb}{b}\right\} && (Q \text{ 中} \odot \text{的定义}) \\
&= \varphi(r) \odot \varphi(s). && (\varphi \text{ 的定义}).
\end{aligned}$$

同时,还有

$$\begin{aligned}
&\varphi(r+s) \\
&\quad = \left\{\frac{(r+s)b}{b}\right\} && (\varphi \text{ 的定义}) \\
&\quad = \left\{\frac{(r+s)bb}{bb}\right\} && (Q \text{ 中元可选不同代表元})
\end{aligned}$$

$$=\left\{\frac{rb}{b}\right\}\#\left\{\frac{sb}{b}\right\} \qquad (Q\text{ 中加法}\#\text{的定义})$$

$$=\varphi(r)\#\varphi(s). \qquad (\varphi\text{ 的定义})$$

这说明 φ 是同态映射.

最后,假设 $\varphi(s)=0_{\#}$,即

$$\left\{\frac{sb}{b}\right\}=\left\{\frac{0}{b}\right\},$$

从而$(sb)b=0$.但 $b\neq 0$,故 $s=0$. $\mathrm{Ker}(\varphi)=\{0\}$, φ 为单射.

综合之,R 在φ之下同构于域Q 的子环 $\mathrm{Img}(\varphi)$.

定理全部证完. ∎

定理 1 的证明是构造性的,读者应先大致掌握构造与证明的大的步骤,心里必须明白,这一步中应该做些什么事.有些非常容易说明的道理,你可以不仔细说,但要明白,这是应该说的,只不过是省略掉了.

例 1 取定理 1 中 R 为整数环 $\mathbf{I}$,元素记为 $m,n,\cdots$.得到域

$$\mathbf{Q}_{\mathrm{I}}=\left\{\left\{\frac{m}{n}\right\},\left\{\frac{k}{l}\right\},\cdots\right\}.$$

我们记有理数环 $\mathbf{Q}$ 的元素为 $m/n,k/l$ 等等.

令

$$\varphi:\left\{\frac{m}{n}\right\}\to m/n.$$

可以证明定义是合理的,即与 $\mathbf{Q}_{\mathrm{I}}$ 中元素代表的选择无关.设

$$\left\{\frac{m}{n}\right\}=\left\{\frac{m'}{n'}\right\}, \quad mn'=m'n.$$

那么,在有理数环中,$m/n=m'/n'$.

同时,对任意整数 m,n,k,l,当 $n\neq 0$, $l\neq 0$ 时

$$\varphi\left(\left\{\frac{m}{n}\right\}\odot\left\{\frac{k}{l}\right\}\right)$$

$$=\varphi\left(\left\{\frac{mk}{nl}\right\}\right) \qquad (\mathbf{Q}_{\mathrm{I}}\text{ 中}\odot\text{的定义})$$

$$\begin{aligned}
&= mk/(nl) && (\varphi \text{ 的定义}) \\
&= (m/n)\cdot(k/l), && (\text{有理数乘法})
\end{aligned}$$

$$\begin{aligned}
&\varphi\left(\left\{\frac{m}{n}\right\} \# \left\{\frac{k}{l}\right\}\right) \\
&= \varphi\left(\left\{\frac{ml+kn}{nl}\right\}\right) && (\mathbf{Q}_1 \text{ 中 } \# \text{ 的定义}) \\
&= (ml+kn)/(nl) && (\varphi \text{ 的定义}) \\
&= m/n + k/l. && (\text{有理数加法})
\end{aligned}$$

所以,φ 是 $\mathbf{Q}_1$ 到 $\mathbf{Q}$ 的环同态映射.

又,由

$$\varphi\left(\left\{\frac{m}{n}\right\}\right) = m/n = 0 \in \mathbf{Q}$$

知必有 $m=0$,即

$$\left\{\frac{m}{n}\right\} = \left\{\frac{0}{n}\right\} = 0_{\#},$$

也就是 $\mathrm{Ker}(\varphi)=\{0_{\#}\}$. φ 为单射. φ 为满射则是显然的事情.

这说明 $\mathbf{Q}_1$ 同构于有理数环 $\mathbf{Q}$.

如果,取定理 1 中的 R 为偶数环 E,$\mathbf{Q}$ 为 $\mathbf{Q}_E$. 同样可以证明,对任意偶数 $m,n,n\neq 0$,规定

$$\psi: \left\{\frac{m}{n}\right\} \to m/n$$

是 $\mathbf{Q}_E$ 到 $\mathbf{Q}$ 的环同态映射,而且是个单射.

任取一有理数 k/l,有

$$\psi\left(\left\{\frac{2k}{2l}\right\}\right) = 2k/(2l) = k/l.$$

这说明 ψ 也是个满射,从而它是个同构映射. $\mathbf{Q}_E$ 也同构于有理数域 $\mathbf{Q}$.

例题 1 设 R 是个无零因子环,且至少含两个元素. Q 是按定理 1 办法构造出来的域 Q. 那么,任意域 F,只要 $R\subseteq F$,则 F

必含一子域Q'同构于Q.

证明 因为F是个域,任取$a,b\in R$, $b\neq 0$,则有$b^{-1}\in F$,从而ab^{-1}在F中是确定的元素.规定,对任意$a\in R$, $b\in R_0$,

$$\varphi:\left\{\frac{a}{b}\right\}\to ab^{-1},$$

即得Q到F的映射.容易验证它是个同态映射,且不是零映射.φ是Q到$\mathrm{Img}(\varphi)$的同构映射,$\mathrm{Img}(\varphi)$是F的子域. ▌

这个例题说明,R如果能嵌入到某域F,那么F必含一同构于Q的子域.也可以说,Q是R可以嵌入的域的最小者(当然是同构意义下讲的).从这种意义上说,Q是由R完全确定的.人们称用这种方法构造出来的这个域Q(以及它的各同构像)为环R的**分式域**或**商域**.

从代数学的观点看,同构的群、同构的环、同构的向量空间的代数结构完全相同,有时索性把同构的代数系统看成是同一个东西.但是,初学者应该清醒地注意到这些区别.

我们约定,给定一个可交换的无零因子环R,它的**分式环**就是

$$Q=\left\{\frac{s}{r}\,\middle|\,s,r\in R,\ r\neq 0\right\}.$$

其运算是

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},\quad \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}.$$

且把Q中元$\left\{\frac{a}{1}\right\}$就记为$\{a\}$.这样一来,就把$Q$的子环

$$R'=\left\{\left\{\frac{a}{1}\right\}\in Q\,\middle|\,a\in R\right\}$$

与环R等同起来,R就成了Q的一个子环.

命题 3 设$R\cong R'$,它们是可交换的无零因子环,Q和Q'分别是它们的分式环,那么,$Q\cong Q'$.

证明 设 φ 是 R 到 R' 的环同构映射. 令

$$\theta: \left\{\frac{a}{b}\right\} \to \left\{\frac{\varphi(a)}{\varphi(b)}\right\}, \quad a, b \in R, \ b \neq 0.$$

首先,当 $b\neq 0$ 时,φ 为同构,$\varphi(b)\neq 0$,从而

$$\left\{\frac{\varphi(a)}{\varphi(b)}\right\}$$

有意义,是 R' 中确定的元素.

其次,要说明定义是合理的. 若

$$\left\{\frac{a}{b}\right\} = \left\{\frac{c}{d}\right\}, \quad ad = bc,$$

则 $\varphi(a)\varphi(d) = \varphi(b)\varphi(c)$,且 $\varphi(b)\neq 0$, $\varphi(d)\neq 0$. 故

$$\left\{\frac{\varphi(a)}{\varphi(b)}\right\} = \left\{\frac{\varphi(c)}{\varphi(d)}\right\}.$$

再次,读者自己可以证明

$$\theta\left(\left\{\frac{a}{b}\right\} + \left\{\frac{c}{d}\right\}\right) = \theta\left(\left\{\frac{a}{b}\right\}\right) + \theta\left(\left\{\frac{c}{d}\right\}\right),$$

$$\theta\left(\left\{\frac{a}{b}\right\}\left\{\frac{c}{d}\right\}\right) = \theta\left(\left\{\frac{a}{b}\right\}\right)\cdot\theta\left(\left\{\frac{c}{d}\right\}\right).$$

最后,可以证明 θ 是个 Q 到 Q' 的双射. 事实上,若

$$\theta\left(\left\{\frac{a}{b}\right\}\right) = \left\{\frac{\varphi(a)}{\varphi(b)}\right\} = \left\{\frac{0'}{1'}\right\},$$

则必有 $\varphi(a) = 0'\varphi(b) = 0'$. 而 φ 是单射,故必有 $a = 0$,这说明 $\left\{\frac{a}{b}\right\}$ 是 Q 的零元. θ 为单射. 对任意

$$\left\{\frac{a'}{b'}\right\} \in Q, \ a', b' \in R', \ b' \neq 0,$$

因 φ 是满射,必有 $a, b \in R$,使 $\varphi(a) = a'$, $\varphi(b) = b'$ 且 $b\neq 0$. 于是

$$\theta\left(\left\{\frac{a}{b}\right\}\right) = \left\{\frac{\varphi(a)}{\varphi(b)}\right\} = \left\{\frac{a'}{b'}\right\},$$

这说明 θ 是满射.

综合之，有 $Q\cong Q'$. ▮

习　题　三

1. 设 R 是个环. 证明：对任意 $r\in R$，如果有 $s\in R$ 使得 $rs=sr$ 且 $r+s+rs=0$，则 s 是由 r 唯一确定的.

2. 如果环 R 是个域，那么 R 的分式域必同构于 R.

3. 设 $R=\{m+n\sqrt{2}\mid m,n\in \mathbf{I}\}$，求它的分式域.

§4　交换环上的多项式

这一节要讨论的多项式环是一类极重要的有单位元的交换环. 之所以说它"重要"是因为，一方面它在数学史上占有显赫地位，另一方面它在解各类方程问题乃至其他学科中有广泛用途.

在初等数学和《数学分析》中，多项式是以函数面目出现的. 函数

$$f(x)=a_0x^n+\cdots+a_{n-1}x+a_n,\quad a_i\in\mathbf{R}$$

中的 x 称为自变量或未知元，等等.

这里要讨论的多项式不限于以数为系数者. 采用"代数方法"定义.

定义 1　设 $(S,+,\cdot)$ 是个有 1 的交换环. 每个形如下面的表达式

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n,$$

（其中 n 为非负整数，$a_0,a_1,\cdots,a_n\in S$）均称为是环 S 上的一个关于 x 的**多项式**.

a_ix^i 称为是多项式 $f(x)$ 的 i 次**项**，a_i 称为 $f(x)$ 的 i 次项**系数**，当 a_i 为 S 中的零元时，表达式中之 i 次项可以不写. a_0 称为**常数项**.

两个多项式说是相等的，当而且仅当，它们的每个同次项系数均相同.

环 S 上所有关于 x 的多项式构成的集合记为 $S[x]$.

可以把 $f(x)$简记为 f.

例 1 $5+6x+\left(-\frac{1}{2}\right)x^2+4x^3$ 是有理数域 **Q** 上关于 x 的一个多项式.

例 2 $1^*+4^*x^2+1^*x^3$ 是环 $\mathbf{I}_5$ 上的一个多项式.

在上述这个文字很多的定义中,关于何谓两个多项式相等的定义至关重要,不可忽视.

例 3 实数域上多项式

$$f(x)=2x^2+2+\sqrt{6}x^3+0x^4,$$

$$g(x)=0x^4+\sqrt{6}x^3+2x^2+0x+2,$$

$$h(x)=\sqrt{6}x^3+2x^2+2$$

是同一个多项式,因为它们每次项的系数均相同,系数为 0 的项可以不写.

读者切不可自作主张用其他办法来衡量两个多项式是否相等. 尤其不可用分析的办法认为"两个多项式相等,当而且仅当,它们是相同的函数".

例 4 在有 1 的交换环 $\mathbf{I}_2=\{0^*,1^*\}$上,多项式

$$f(x)=1^*x^4+1^*x,$$

$$g(x)=1^*x^2+1^*x,$$

$$h(x)=0^*x+0^*,$$

是两两不同的多项式. 尽管作为"函数",有

$$f(0^*)=0^*,\quad f(1^*)=0^*,$$

$$g(0^*)=0^*,\quad g(1^*)=0^*,$$

$$h(0^*)=0^*,\quad h(1^*)=0^*,$$

也就是说,即使它们"处处相等",也绝不可认为

$$f(x)=g(x)=h(x).$$

那么,本课程所定义的多项式概念与"传统意义"不是发生予

盾了吗？后面将说明，在数域上，“代数的”定义和“分析的”定义是一致的，新引进的多项式概念是原来已经知道的多项式概念的推广.

定义 2 设 S 是个有 1 的交换环. 如果多项式

$$f(x)=a_0+a_1x+\cdots+a_nx^n,$$
$$g(x)=b_0+b_1x+\cdots+b_mx^m,$$

其中 $m\geqslant n$. 那么，规定多项式

$$(a_0+b_0)+(a_1+b_1)x+\cdots+(a_n+b_n)x^n+b_{n+1}x^{n+1}+\cdots+b_mx^m$$

为 $f(x)$与 $g(x)$的**和**，记为 $f(x)+g(x)$.

规定多项式

$$a_0b_0+(a_1b_0+a_0b_1)x+\cdots+a_nb_mx^{m+n}$$

为 $f(x)$与 $g(x)$的**乘积**，记为 $f(x)g(x)$.

例 5 在 I 上，

$$(6+3x+5x^2)+[(-3)+x^2+(-2)x^3]=3+3x+6x^2+(-2)x^3,$$
$$(3+7x^3)+(-3)+1x^2=1x^2+7x^3,$$
$$(1+1x)[1+(-1)x]=1+(-1)x^2.$$

例 6 在 I_6 上

$$(1^*x+2^*x^2)+(1^*+4^*x^2)=1^*+1^*x,$$
$$(1^*x+2^*x^2)(3^*x^2)=3^*x^3.$$

定理 1 设 S 是个有 1 的交换环，那么，$S[x]$在上面规定的多项式的加法和乘法之下作成一个有 1 的交换环.

证明 $S[x]$关于加法满足结合律和交换律的验证是很容易的. 多项式

$$0=0+0x=0+0x+\cdots+0x^n=\cdots$$

就是$(S[x],+,\cdot)$的加法零元素，通称零多项式.

对于 $f(x)=a_0+a_1x+\cdots+a_nx^n$，多项式

$$g(x)=(-a_0)+(-a_1)x+\cdots+(-a_n)x^n$$

恰为 $f(x)$的负元素.

关于分配律和乘法交换律的验证也是比较容易的.现在来验证乘法结合律.设

$$f(x)=a_0+a_1x+\cdots+a_nx^n,$$
$$g(x)=b_0+b_1x+\cdots+b_mx^m,$$
$$h(x)=c_0+c_1x+\cdots+c_px^p,$$
$$f(x)g(x)=d_0+d_1x+\cdots+d_kx^k,$$
$$g(x)h(x)=e_0+e_1x+\cdots+e_lx^l.$$

按定义,要证明$[f(x)g(x)]h(x)=f(x)[g(x)h(x)]$,必要而且只要验证它们同次项的系数相同.

多项式$[f(x)g(x)]h(x)$之第 i 项的系数是

$$d_0c_i+d_1c_{i-1}+\cdots+d_ic_0=\sum_{j=0}^{i}d_jc_{i-j}, \tag{1}$$

而每个 d_j 乃是$f(x)g(x)$之第 j 项系数,故

$$d_j=a_0b_j+\cdots+a_jb_0=\sum_{t=0}^{j}a_tb_{j-t}. \tag{2}$$

将(2)代入(1),得

$$\sum_{j=0}^{i}\sum_{t=0}^{j}a_tb_{j-t}c_{i-j}. \tag{3}$$

实际上,它就是 a_u, b_v 和 c_w 的所有脚码之和为 i 的积 $a_ub_vc_w$ 之和,即(3)等于

$$\sum_{u+v+w=i}a_ub_vc_w. \tag{4}$$

多项式 $f(x)[g(x)h(x)]$之第 i 项的系数是

$$\sum_{q=0}^{i}a_{i-q}e_q. \tag{5}$$

而 $e_q=\sum_{s=0}^{q}b_sc_{q-s}$,从而可算出(5)等于

$$\sum_{q=0}^{i}\sum_{s=0}^{q}a_{i-q}b_sc_{q-s}. \tag{6}$$

它也恰好是取尽 3 个脚码之和为 i 之各种可能的 a_u, b_v 和 c_w 的

积再做的和.所以,(6)和(4)是一致的.

多项式 $1x=0+1x+\cdots+0x^n$ 就是 $S[x]$ 的恒等元.

$S[x]$ 在 $+$ 和 $\cdot$ 之下是个有 1 的交换环. ▎

定义 3 环 $(S[x],+,\cdot)$ 称为环 S 上关于 x 的**多项式环**.

定义 4 多项式

$$f(x)=a_0+a_1x+\cdots+a_nx^n+\cdots+a_mx^m$$

中,如果 $a_n\neq 0$,而 $a_{n+1}=\cdots=a_m=0$,则说 $f(x)$ 的次数为 n,记为

$$\deg f(x)=n.$$

零多项式的次数用符号 $-\infty$ 来记.这样,每个多项式都有次数了.为说话方便,还规定对任意非负整数 n,

$$-\infty<n,\ (-\infty)+(-\infty)=-\infty,\ -\infty+n=-\infty.$$

命题 1 对任意 $f(x),g(x)\in S[x]$,恒有

$$\deg[f(x)+g(x)]\leqslant\max\{\deg f(x),\deg g(x)\},$$
$$\deg[f(x)g(x)]\leqslant\deg f(x)+\deg g(x),$$

其中 $\max\{m,n\}$ 代表两数 m,n 之最大者.

证明 设

$$\begin{aligned}f(x)&=a_0+a_1x+\cdots+a_nx^n,\\ g(x)&=b_0+b_1x+\cdots+b_mx^m.\end{aligned}\tag{7}$$

当它们有一个为零多项式时,命题显然是对的.现假定 $f(x)$ 和 $g(x)$ 均不为零多项式.它们的次数分别为 p 和 q.

看 $f(x)+g(x)$ 的 i 次项系数.若 $i>p,q$,那么 $a_i=0$, $b_i=0$.故 $a_i+b_i=0$.故

$$\deg[f(x)+g(x)]\leqslant p,q.$$

再看 $f(x)g(x)$ 的 j 次项系数.若 $j>p+q$,那么,对任意 $t\leqslant j$,必有 $t>p$ 或 $j-t>q$.故

$$\sum_{t=0}^{j}a_tb_{j-t}=0.$$

从而 $\deg[f(x)g(x)]\leqslant p+q$. ▌

推论 当 S 是整环时，$S[x]$ 亦为整环. ▌

事实上，若 $f(x),g(x)$ 均不为零多项式，设在(7)中，$a_p\neq 0$, $a_i=0$,对所有 $i>p$; $b_q\neq 0$, $b_j=0$,对所有 $j>q$. 于是

$$\sum_{i+j=p+q} a_i b_j$$

中只有 $a_p b_q\neq 0$,其余各项均为 0. 也就是说，$f(x)g(x)$ 的第 $p+q$ 项 $a_p b_q$ 不为 0.

命题 2 设 R 是个有 1 的交换环，$R[x]$ 是 R 上关于 x 的多项式环. 那么，取定 $u\in R$ 时，

$$\varphi: a_0+a_1x+\cdots+a_nx^n \to a_0+a_1u+\cdots+a_nu^n$$

是环 $R[x]$ 到 R 的环同态映射.

证明 显然，映射 φ 的定义是合理的，多项式的表达式中差若干个以 0 为系数的项不影响对应的结果.

任取 $f(x),g(x)\in R[x]$,如(7).有

$$\begin{aligned}
&\varphi[f(x)+g(x)]\\
&\quad=\varphi[(a_0+b_0)+(a_1+b_1)x+\cdots] && (R[x]\text{的加法})\\
&\quad=(a_0+b_0)+(a_1+b_1)u+\cdots && (\varphi\text{ 的定义})\\
&\quad=(a_0+a_1u+\cdots+a_nu^n)+(b_0+\cdots+b_mu^m) && (R\text{ 中的加法})\\
&\quad=\varphi[f(x)]+\varphi[g(x)], && (\varphi\text{ 的定义})\\
&\varphi[f(x)g(x)]\\
&\quad=\varphi[a_0b_0+(a_0b_1+a_1b_0)x+\cdots] && (R[x]\text{的乘积})\\
&\quad=a_0b_0+(a_0b_1+a_1b_0)u+\cdots+a_nb_mu^{m+n} && (\varphi\text{ 的定义})\\
&\quad=(a_0+\cdots+a_nu^n)(b_0+\cdots+b_mu^m) && (R\text{ 的乘积})\\
&\quad=\varphi[f(x)]\varphi[g(x)], && (\varphi\text{ 的定义})
\end{aligned}$$

所以，φ 是 $R[x]$ 到 R 的环同态. ▌

我们记

$$\varphi[f(x)]=a_0+a_1u+\cdots+a_nu^n=f(u).$$

命题 2 证明了

$$(f+g)(u)=f(u)+g(u),$$
$$(fg)(u)=f(u)g(u).$$

定义 5 设 S 是有 1 交换环，$f(x)\in S[x]$. 说元素 $r\in S$ 是多项式 $f(x)$ 的一个根，如果 $f(r)=0$. 也可以说 r 满足多项式 $f(x)$.

例如，1 是有理数域上多项式

$$f(x)=1x^2+(-1)$$

的一个根，-1 也是该多项式的根.

环 $\mathbf{I}_3\oplus\mathbf{I}_3$ 上的 2 次多项式

$$g(x)=(1^*,1^*)x^2+(2^*,2^*)$$

有 4 个根，它们是

$$(1^*,1^*),(1^*,2^*),(2^*,1^*),(2^*,2^*).$$

下面，我们来讨论这样一个问题，设 S 是环 R 的一个子环，$r\in R$. 问，R 中由集合

$$S\cup\{r\}$$

生成的子环 $\langle S\cup\{r\}\rangle$ 是什么样子.

注意，有 1 环的子环未必有 1，如果子环有恒等元，也未必与大环的恒等元一致.

例如，偶数环 E 和整数环 $\mathbf{I}$ 的外直和 $E\oplus\mathbf{I}$ 中，$E\oplus\mathbf{I}$ 无恒等元，但它的子环 $\bar{\mathbf{I}}=\{(0,n)\mid n\in\mathbf{I}\}$ 有恒等元.

$\mathbf{I}$ 有恒等元，而其子环 E 无恒等元.

$\mathbf{I}\oplus\mathbf{I}$ 有恒等元 $(1,1)$，子环

$$\bar{\mathbf{I}}=\{(0,n)\mid n\in\mathbf{I}\}$$

亦有恒等元 $(0,1)$，但二者并不相等.

注意这点以后，就可以证明下面的

命题 3 设 R 是个有 1 的交换环，S 是 R 的子环且有(自己的)恒等元，$r\in R$. 如果 r 不是 $S[x]$ 中任何非零多项式的根，那么

$$\langle S\cup\{r\}\rangle\cong S[x]\}.$$

证明 建立映射 $\varphi: f(x) \to f(r)$，这是 $S[x]$ 到 R 的映射.

若 $f(x) \in S[x]$，设

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n, \quad a_i \in S,$$

那么，由于 $\langle S \cup \{r\} \rangle$ 是含 S 又含 r 的子环，故

$$f(r) = a_0 + a_1 r + \cdots + a_n r^n \in \langle S \cup \{r\} \rangle.$$

也就是说 $\mathrm{Img}(\varphi) \subseteq \langle S \cup \{r\} \rangle$.

另一方面，$\mathrm{Img}(\varphi)$ 是一个环的同态像，它本身是个环，也就是说 $\mathrm{Img}(\varphi)$ 是 R 的子环. 而且 S 中每个元 s 就是一个关于 x 的常数多项式，记 $h(x) = s$，则 $h(r) = s$，从而 $s \in \mathrm{Img}(\varphi)$. 也就是

$$S \subseteq \mathrm{Img}(\varphi).$$

再看多项式 $i(x) = 1x$，由 $i(r) = 1r = r$ 知 $r \in \mathrm{Img}(\varphi)$.

所以，R 的子环 $\mathrm{Img}(\varphi)$ 既包含 S 又包含了元素 r. 从而 $\langle S \cup \{r\} \rangle \subseteq \mathrm{Img}(\varphi)$. 进而 $\langle S \cup \{r\} \rangle = \mathrm{Img}(\varphi)$.

研究 $\mathrm{Ker}(\varphi)$. 如果 $f(x) \in S[x]$ 使 $\varphi[f(x)] = 0$，即 $f(r) = 0$. 但，r 不是任何 S 上非零多项式的根. 故 $f(x)$ 只能是零多项式，也就是 $S[x]$ 的零元素，即 $\mathrm{Ker}(\varphi) = \{0\}$.

由环同态基本定理，得

$$S[x]/\mathrm{Ker}(\varphi) \cong S[x] \cong \mathrm{Img}(\varphi) = \langle S \cup \{r\} \rangle. \qquad \blacksquare$$

命题 3 告诉我们，多项式的定义虽然有些抽象，但它代表的东西还是相当具体的，$S[x]$ 实际上是在环 S 上又添上了另外一个元素所得到的一个新的比较大的环. 不过新添的元素与 S 关系相当“疏远”.

例如，在实数域 $\mathbf{R}$ 中，自然对数底 e 和圆周率 π 都是所谓超越数，人们已经证明，它们都不是任何非零有理多项式的根. 所以

$$\mathbf{I}[x] \cong \langle \mathbf{I} \cup \{\mathrm{e}\} \rangle \cong \langle \mathbf{I} \cup \{\pi\} \rangle.$$

而实数 $\sqrt{2}$ 与整数环 $\mathbf{I}$ 的关系就不那么“疏远”，它满足非零整系数多项式

$$1x^2 + (-2),$$

$\langle \mathbf{I} \cup \{\sqrt{2}\}\rangle$之结构又当别论.

本书后面,常把多项式中的系数 1 省去不记,$(-a)x^i$ 直接记为 $-ax^i$. 例如 $1x^2+(-2)=x^2-2$.

下面,我们对域 F 上的多项式环 $F[x]$做进一步讨论.

命题 4 设 F 是个域,$f(x),g(x)\in F[x]$. 那么

$$\deg[f(x)g(x)]=\deg f(x)+\deg g(x).$$

这是命题 1 推论证明中的特殊情形. ▌

定义 6 设 D 是个整环,多项式

$$f(x)=a_0+a_1x+\cdots+a_rx^r+\cdots+a_nx^n,\ a_i\in D,$$

中,$a_r\neq 0$,且当 $j>r$ 时有 $a_j=0$,即 $\deg f=r$,则说 a_r 是$f(x)$的**首系数**.

多项式也可以采用所谓降幂排列法,例如上面给定的多项式 $f(x)$也可以写成

$$f(x)=a_rx^r+\cdots+a_1x+a_0.$$

命题 5 设 D 是个整环. $f(x)\in D[x]$, $g(x)$是 $D[x]$中首系数为 1 的多项式. 那么,必有 $q(x),r(x)\in D[x]$使

$$f(x)=g(x)q(x)+r(x),\quad \deg r(x)<\deg g(x).$$

证明 如果我们已经有 $\deg f(x)<\deg g(x)$,只要取 $q(x)=0$, $r(x)=f(x)$,就有

$$f(x)=0g(x)+f(x),\quad \deg f(x)<\deg g(x).$$

现假定

$$f(x)=a_mx^m+\cdots+a_1x+a_0,\quad a_m\neq 0,$$

$$g(x)=x^n+\cdots+b_1x+b_0,$$

$d=m-n\geqslant 0$. 对 d 用数学归纳法.

当 $d=0$ 时,

$$f(x)=g(x)a_n+[(a_{n-1}-b_{n-1}a_n)x^{n-1}+\cdots+(a_0-b_0a_n)],$$

符合命题要求.

现在假定,命题对满足 $\deg f(x)-\deg g(x)<d$ 的$f(x)$都是

对的，令

$$f(x)=g(x)\cdot a_m x^{m-n}+h(x),$$

显然，$\deg h(x)\leqslant m-1$. 当 $\deg h(x)<n$ 时，命题真确；当 $\deg h(x)\geqslant n$ 时，有

$$\deg h(x)-\deg g(x)<d.$$

由归纳法假定，应有 $q(x),r(x)$ 使

$$h(x)=g(x)q(x)+r(x),\quad \deg r(x)<\deg g(x).$$

也就是

$$f(x)-g(x)\cdot a_m x^{m-n}=g(x)q(x)+r(x),$$

$$f(x)=g(x)[q(x)+a_m x^{m-n}]+r(x),$$

而且 $\deg r(x)<\deg g(x)$.

命题得证. ▌

定理 2 设 F 是个域. 那么，对任意 $f(x),g(x)\in F[x]$，只要 $g(x)\neq 0$，必有 $q(x),r(x)\in F[x]$ 使得

$$f(x)=g(x)q(x)+r(x),\quad \deg r(x)<\deg g(x).\quad (*)$$

其中 $\deg r(x)<\deg g(x)$ 包括了 $r(x)=0$ 或 $r(x)$ 次数小于 $g(x)$ 次数两情形.

进一步，满足(*)的 $q(x)$ 和 $r(x)$ 是由 $f(x)$ 完全决定的.

证明 设

$$g(x)=b_n x^n+\cdots+b_1x+b_0,\quad b_n\neq 0.$$

由于 F 是个域，$b_n\neq 0$ 则必有逆. 看多项式

$$g^*(x)=b_n^{-1}g(x)=x^n+\cdots+b_n^{-1}b_0,$$

它的首项系数为 1，由命题 5，必有 $q(x),r(x)\in F[x]$ 使

$$f(x)=q^*(x)g^*(x)+r(x),\quad \deg r(x)<\deg g^*(x).$$

而 $\deg g^*(x)=\deg g(x)$，故有

$$f(x)=g(x)[b_n^{-1}q^*(x)]+r(x),\quad \deg r(x)<\deg g(x).$$

取 $q(x)=b_n^{-1}q^*(x)$，即有

$$f(x)=g(x)q(x)+r(x),\quad \deg r(x)<\deg g(x).$$

进一步，设又有 $q_1(x), r_1(x)$ 使

$$f(x)=g(x)q_1(x)+r_1(x), \quad \deg r_1(x)<\deg g(x). \quad (**)$$

将(*)和(**)两端分别相减，得

$$g(x)(q(x)-q_1(x))=r_1(x)-r(x).$$

比较其两端多项式的次数，若 $q(x)-q_1(x)$ 不是零多项式，则

$$\deg g(x)\leqslant\deg(r_1(x)-r(x))\leqslant\max\{\deg r_1(x),\deg r(x)\},$$

矛盾.

所以，$q_1(x)-q(x)=0$，进而 $r_1(x)-r(x)=0$，即

$$q(x)=q_1(x), r(x)=r_1(x). \quad ▌$$

命题 5 和定理 1 的证明写出来要说很多话，表面上相当复杂. 而实际上，它们是初等数学中数域上的多项式带余除法(或称长除法)的推广，理解起来并不难.

例如，在有理数域 Q 上，取

$$f(x)=x^3+x+1, \quad g(x)=x-2.$$

用 $g(x)$ 去除 $f(x)$ 的步骤是

$$\begin{array}{r|l}
 & x^2+2x+5 \\ \hline
x-2 & x^3 \qquad\quad +x+1 \\
 & x^3-2x^2 \\ \hline
 & \quad 2x^2+x \\
 & \quad 2x^2-4x \\ \hline
 & \qquad 5x+1 \\
 & \qquad 5x-10 \\ \hline
 & \qquad\quad 11
\end{array}$$

得

$$q(x)=x^2+2x+5, \quad r(x)=11,$$

$$(x^3+x+1)=(x-2)(x^2+2x+5)+11.$$

定理 3 设 F 是个域. 那么，环 $F[x]$ 的每个理想都是一个主理想.

证明 设 I 是 $F[x]$ 的一个理想.

如果 $I=\{0\}$，那么 I 就是元素 0 生成的主理想.

如果 $I\neq\{0\}$，设 $g(x)$是 I 中所有非零多项式中次数最低者之一. 可以断言 $g(x)$生成的主理想$(g(x))$恰好等于理想 I.

一方面，$g(x)\in I$，故$(g(x))\subseteq I$.

另一方面，任取 $f(x)\in I$. 据定理 1，必有 $q(x)$，$r(x)\in F[x]$使得

$$f(x)=g(x)q(x)+r(x),\quad \deg r(x)<\deg g(x).$$

又 $f(x)\in I$，$g(x)\in I$，$g(x)q(x)\in I$，故 $r(x)\in I$.

但是，$g(x)$是 I 里所有非零多项式中具有最低次数者. $\deg r(x)<\deg g(x)$导致 $r(x)$必须为零多项式. 从而

$$f(x)=q(x)g(x)\in I.$$

这说明 $I\subseteq(g(x))$.

总之，有 $I=(g(x))$. ▎

例题 1 设 F 是个域，$f(x)\in F[x]$，$c\in F$. 那么，必有 $q(x)\in F[x]$使得$f(x)=q(x)(x-c)+f(c)$.

证明 用多项式 $x-c$ 除 $f(x)$，由于 $\deg(x-c)=1$，必有 $q(x)$，$r(x)\in F[x]$，使

$$f(x)=q(x)(x-c)+r(x),\quad 次数\ r(x)<1.$$

从而 $r(x)$或为 0 或为零次多项式(即非零的常数多项式). 设 $r(x)=a\in F$，则

$$f(x)=q(x)(x-c)+a.$$

上式之两端均用 c 代入，有

$$f(c)=q(c)(c-c)+a=a,$$

也就是 $f(x)=q(x)(x-c)+f(c)$. ▎

举个具体的例子. 数域 $\mathbf{I}_5$ 上，设

$$f(x)=2^*x^4+1^*x+3^*.$$

那么，$f(2^*)=2^*\cdot1^*+2^*+3^*=2^*$. 做除法

$$
\begin{array}{r|l}
 & 2^* x^3 + 4^* x^2 + 3^* x \\
\hline
1^* x - 2^* & 2^* x^4 \qquad\qquad\qquad\qquad + 1^* x + 3^* \\
 & \underline{2^* x^4 - 4^* x^3} \\
 & \qquad 4^* x^3 \\
 & \qquad \underline{4^* x^3 - 3^* x^2} \\
 & \qquad\qquad 3^* x^2 + 1^* x \\
 & \qquad\qquad \underline{3^* x^2 - 1^* x} \\
 & \qquad\qquad\qquad 2^* x + 3^* \\
 & \qquad\qquad\qquad \underline{2^* x - 4^*} \\
 & \qquad\qquad\qquad\qquad 7^*
\end{array}
$$

所得之余数也是 7^*.

命题 6 设 F 是个域, $f(x) \in F[x]$, $a \in F$. 那么, a 是 $f(x)$ 的根, 当而且仅当 $x-a$ 整除 $f(x)$.

证明 若 $x-a$ 能整除 $f(x)$, 有 $g(x) \in F[x]$ 使

$$f(x) = g(x)(x-a),$$

那么, $f(a) = g(a)(a-a) = 0$, a 是 $f(x)$ 的一个根.

反之, 若 a 是 $f(x)$ 的一个根, 做除法

$$f(x) = g(x)(x-a) + r,$$

因为 $x-a$ 是一次多项式, 故 r 为 0 次或 $-\infty$ 次, 即 $r=0$ 或 r 为 F 中非 0 元素. 将 a 代入除式, 得

$$r + g(a)(a-a) = f(a) = 0.$$

故知 $r=0$, $f(x) = g(x)(x-a)$, 也就是 $x-a$ 能够整除 $f(x)$. ∎

命题 7 设 $f(x)$ 是域 F 上的 n 次多项式, $n \geq 1$. 那么, F 中至多有 n 个不同的元素是 $f(x)$ 的根.

证明 设 $a_1, \cdots, a_t \in F$, 两两不同, 它们都是 $f(x)$ 的根.

首先, a_1 是 $f(x)$ 的根, 据命题 6, 应有

$$f(x) = (x - a_1) g(x).$$

将 a_2 代入 $f(x)$, 因 a_2 是它的一个根, 故有

$$0 = f(a_2) = (a_2 - a_1) g(a_2).$$

而 $a_1 \neq a_2$, 从而必有 $g(a_2) = 0$.

于是，由 a_2 为 $g(x)$ 的根推知

$$g(x)=(x-a_2)h(x),\quad f(x)=(x-a_1)(x-a_2)h(x).$$

这样不断做下去，就有

$$f(x)=(x-a_1)(x-a_2)\cdots(x-a_t)k(x).$$

由于 $(x-a_1)\cdots(x-a_t)$ 的次数 t 不能大于 n，即得结论． ▌

命题 7 对于数域上成立是大家早就知道的了，而对一般有 1 可换环此事不真．本节开头就讲了，$\mathbf{I}_3\oplus\mathbf{I}_3$ 上一个二次多项式有 4 个根．

例题 2 设 F 是个域，$a_1,a_2,\cdots,a_n$ 是 F 中 n 个不同的元素；而 $b_1,b_2,\cdots,b_n$ 是 F 中任意 n 个元素．令

$$p_i(x)=(x-a_1)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_n),$$
$$i=1,2,\cdots,n.$$

那么，显然有 $p_i(a_i)\neq 0$．再令

$$f(x)=\sum_{i=1}^{n}\frac{b_i}{p_i(a_i)}p_i(x),$$

则 $f(x)$ 是域 F 上次数不大于 $n-1$ 的唯一的一个使

$$f(a_1)=b_1,\ f(a_2)=b_2,\ \cdots,\ f(a_n)=b_n$$

的多项式．

证明 由于 $j\neq i$ 时，$p_i(a_j)=0$，故显然有

$$f(a_i)=b_i,\quad i=1,2,\cdots,n.$$

如果又有次数不大于 $n-1$ 的多项式 $g(x)$ 使

$$g(a_i)=b_i,\quad i=1,2,\cdots,n.$$

那么，多项式 $h(x)=f(x)-g(x)$ 次数亦不大于 $n-1$．但

$$h(a_i)=f(a_i)-g(a_i)=b_i-b_i=0,$$

说明 $h(x)$ 有 n 个不同的根．据命题 7，$h(x)$ 必然是零多项式，即 $f(x)-g(x)=0$；也就是 $f(x)=g(x)$． ▌

例题 3 有理数域 $\mathbf{Q}$ 上多项式 $f(x)$ 和 $g(x)$ 相等，当而且仅当，对任意 $a\in\mathbf{Q}$，有 $f(a)=g(a)$．

证明 若 $f(x)=g(x)$,那么,对任意 $a\in\mathbf{Q}$,当然有

$$f(a)=g(a).$$

反之,设 $f(x)-g(x)$的次数为 n,若对任意 a 恒有$f(a)=g(a)$,即

$$f(a)-g(a)=0,$$

$f(x)-g(x)$有多于 n 个根,它只能是零多项式,从而得

$$f(x)=g(x).$$ ▌

这个例题解决了本节开头提出的问题,我们定义的多项式概念,在有理数域、实数域等上面,与《数学分析》多项式函数概念一致.

命题 8 设 F 是个域,

$$f(x)=a_0+a_1x+\cdots+a_nx^n,\quad a_n\neq 0,$$

I 是$f(x)$在 $F[x]$中生成的主理想.那么,剩余环 $F[x]/I$ 的每个元素均可唯一地表成如下形式

$$(b_0+b_1x+\cdots+b_{n-1}x^{n-1})+I, b_0, b_1\cdots b_{n-1}\in F,\quad (*)$$

而且

$$F'=\{b+I\mid b\in F\}$$

是 $F[x]/I$ 的子域,它同构于 F.

证明 任取 $F[x]/I$ 的元素$g(x)+I$,其中 $g(x)\in F[x]$.用 $f(x)$除之,必有 $q(x), r(x)\in F[x]$,

$$g(x)=f(x)q(x)+r(x),\quad \deg r(x)<\deg f(x)=n.$$

由于

$$g(x)-r(x)=f(x)q(x)\in I,$$

故

$$g(x)+I=r(x)+I,$$

从而 $F[x]/I$ 的元素至少有一种方法表成($*$)形式.

另一方面,如果

$$b_0+b_1x+\cdots+b_{n-1}x^{n-1}+I=c_0+c_1x+\cdots+c_{n-1}x^{n-1}+I$$

那么,

$$(b_0-c_0)+(b_1-c_1)x+\cdots+(b_{n-1}-c_{n-1})x^{n-1}\in I.$$

所以，$f(x)$要整除一个次数小于 n 的多项式

$$(b_0-c_0)+(b_1-c_1)x+\cdots+(b_{n-1}-c_{n-1})x^{n-1}.$$

从而，上面这个多项式必然为0.得到

$$b_0=c_0,\ b_1=c_1,\ \cdots,\ b_{n-1}=c_{n-1},$$

这就证明了唯一性.

令 $\varphi: b \to b+I$ 则得到 F 到 F' 的一个映射.很容易说明这是个同构映射. ▌

现在，可以回过头来审视一下，多项式

$$f(x)=a_0+a_1x+\cdots+a_nx^n$$

中这个"x"到底是个什么东西.

严格说来，在抽象代数学中，称其为变元或不变量是不恰当的，因为多项式不是在任何环上都能作为"函数"来讨论的.

称 x 为未知量也不合适，因为，并不是一定要把这个 x 求出来使其为已知的某元.

实际上，在多项式中关键是它的各个系数，$1,x,x^2,\cdots,x^n$ 只起标记系数位置的作用.在整个讨论中，究竟是用 x 还是用 y，抑或是用 λ 都是无关紧要的.

因此，简简单单地称 x 为"文字"比较恰当.但，有些书沿用初等代数语言称 x 为变元或变量，我们不可按字面理解.

在代数同构的观点之下，可以完全不出现任何"文字"而照样讨论多项式环.

例题 4 设 S 是个有 1 的交换环.考虑 S 上所有(元素)序列，

$$f=(a_0,a_1,\cdots,a_n,\cdots),\quad a_i\in S,\ a_{n+1}=a_{n+2}=\cdots=0,$$

的集合 $S[\ ]$.规定，二序列相等，当而且仅当，它们对应的项均相等.

对任意二序列

$$g=(b_0,b_1,\cdots,b_m,\cdots),\quad b_j\in S,\ b_{m+1}=b_{m+2}=\cdots=0,$$
$$f=(a_0,a_1,\cdots,a_m,\cdots),\quad a_i\in S,\ a_{m+1}=a_{m+2}=\cdots=0,$$
规定序列
$$(a_0+b_0,\cdots,a_m+b_m,\cdots)$$
为 f 与 g 的和,记为 $f+g$ 规定,序列
$$(a_0b_0,a_1b_0+a_0b_1,\cdots,a_0b_m+a_1b_{m-1}+\cdots+a_mb_0,\cdots)$$
与 f 与 g 的积,且记为 $f\cdot g$.

那么,$(S[\,],+,\cdot)$作成一个环,它同构于环 $S[x]$.

证明 建立映射 φ,
$$\varphi:(a_0,a_1,\cdots,a_n,\cdots)\mapsto a_0+a_1x+\cdots+a_nx^n,$$
由于序列只有有限项不为 0,多项式
$$a_0+a_1x+\cdots+a_nx^n$$
中以 0 为系数者又可写可不写,所以它是由序列$(a_0,a_1,\cdots,a_n\cdots)$唯一确定的. φ 是$S[\,]$到环 $S[x]$的映射.

不同的序列必至少有某对应项不同,从而它们对应的多项式有某对应项系数亦不同. 这说明 φ 是个单射.

容易说明,φ 是个满射,从而 φ 是个双射.

再进一步,据 $S[\,]$的加法和乘法定义可以看出,对任意 $f,g\in S[\,]$,还有
$$\varphi(f+g)=\varphi(f)+\varphi(g),$$
$$\varphi(f\cdot g)=\varphi(f)\varphi(g).$$

由第四章§4之例题 6 知道 $S[\,]$必然是个环而且它同构于多项式环 $S[x]$. ▌

这个例题说明多项式理论中文字 x 可任意选择甚至索性不用任何文字,关键是各系数的位置.

但是,用序列记多项式具体运算起来也有不方便之处,本书仍择一文字记之.

我们再介绍些多文字多项式知识,它是研究域扩张(第七章)

的重要工具.

定义 7 设 R 是个有 1 的交换环. 形式表达式

$$f(x,y)=a_{0,0}+a_{1,0}x+a_{0,1}y+a_{2,0}x^2+a_{0,2}y^2+a_{1,1}xy+\cdots+a_{n,0}x^n+a_{n-1,1}x^{n-1}y+\cdots+a_{0,n}y^n,\ a_{ij}\in R,$$

称为 R 上关于文字 x,y 的**二元多项式**.

$a_{ij}x^iy^j$ 称为 x 的 i 次、y 的 j 次项, 而 a_{ij} 称为 x 的 i 次、y 的 j 次项系数.

规定, 等于 0 的系数可以不写出来; 多项式

$$f(x,y) = \sum a_{ij}x^iy^j, \tag{7}$$

$$g(x,y) = \sum b_{ij}x^iy^j, \tag{8}$$

相等, 当而且仅当, 它们对应的系数逐项相同, 即

$$a_{ij}=b_{ij} \quad (i,j=0,1,\cdots);$$

任意两个多项式 $f(x,y)$, $g(x,y)$ 如(7), (8), 它们的和是

$$\sum (a_{ij}+b_{ij})x^iy^j.$$

记为 $f(x,y)+g(x,y)$; 它们的积是 $\sum c_{ij}x^iy^j$, 其中

$$c_{ij}=\sum_{\substack{s+p=i\\ t+q=j}} a_{st}b_{pq},$$

也就是先做形式积 $\sum a_{st}b_{pq}x^sx^py^ty^q$, 然后把"含 x,y 个数"完全相同的项合起来, 即得其积的各系数.

不难验证, F 上关于文字 x,y 的所有多项式的集合, 在上面定义的加法和乘法之下构成一个环, 记为 $F[x,y]$.

注意, 对任意 $f(x,y)\in F[x,y]$, 表达式

$$f(x,y)=a_{0,0}+a_{1,0}x+a_{0,1}y+\cdots+a_{ij}x^iy^j+\cdots$$

又可以看成是多项式

$$a_{0,0},a_{1,0}x,\cdots,a_{ij}x^iy^j$$

之和, 而 $a_{ij}x^iy^j$ 又可以看成是多项式

$$a_{ij}x^i, y^j$$

的乘积，x^i 和 y^j 是可换的，即 $x^iy^j=y^jx^i$.

现在研究这样一个问题：设 F 是个域. 那么 F 上关于文字 x 的多项式构成环 $F[x]$，它是个有 1 可交换的无零因子环. 又可以讨论 $F[x]$ 上关于文字 y 的所有多项式构成的环 $F[x][y]$，它的元素形如

$$k(y)=p_0+p_1y+\cdots+p_ny^n,$$

其中 $p_0,p_1,\cdots,p_n\in F[x]$. 那么，环 $F[x][y]$ 和环 $F[x,y]$ 有关系吗？

定理 4 设 F 是个域，那么环 $F[x][y]$ 和环 $F[x,y]$ 同构.

证明 任取

$$k(y)=p_0(x)+p_1(x)y+\cdots+p_n(x)y^n,$$

$$p_i(x)=a_{i0}+a_{i1}x+\cdots+a_{im}x^m,\quad i=0,\cdots,n.$$

令它对应

$$f(x,y)=a_{00}+a_{10}x+a_{01}y+\cdots+a_{mn}x^my^n,$$

这是 $F[x][y]$ 到 $F[x,y]$ 的一个映射，记为 φ.

首先，φ 是个满射，对任意 $f(x,y)\in F[x,y]$，它的各项书写顺序是可以任意变动的，现将 $f(x,y)$ 先按 y 的升幂合并，写成

$$f(x,y)=\sum a_ix^i+\sum b_jx^jy+\cdots+\sum c_lx^ly^n.$$

那么，

$$\varphi\Big(\big(\sum a_ix^i\big)+\big(\sum b_jx^j\big)y+\cdots+\big(\sum c_lx^l\big)y^n\Big)=f(x,y).$$

其次，φ 显然是个单射.

再次，对任意

$$k(y)=p_0(x)+p_1(x)y+\cdots+p_m(x)y^m,\tag{9}$$

$$h(y)=q_0(x)+q_1(x)y+\cdots+q_m(x)y^m,\tag{10}$$

很容易验证，有

$$\varphi[k(y)+h(y)]=\varphi[k(y)]+\varphi[h(y)].$$

因为不管是在 $F[x][y]$ 中还是在 $F[x,y]$ 中，系数为 0 的项

可以随便添写.故可以把(9),(10)中出现的 y 的项写到 m 项,同时可要求

$$p_0(x), p_1(x), \cdots, p_m(x),$$
$$q_0(x), q_1(x), \cdots, q_m(x)$$

的 x 项都写到 n 次.

最后,对任意 $k(y), h(y) \in F[x][y]$ 如(9)和(10),可以验证

$$\varphi[k(y)h(y)] = \varphi[k(y)]\varphi[h(y)].$$

按定义,只需验证等式两端多项式之 x 的 i 次项、y 的 j 次项均相同($i, j = 0, 1, 2, \cdots$).

左端

$$k(y)h(y) = \cdots + [p_0(x)q_j(x) + \cdots + p_j(x)q_0(x)]y^j + \cdots,$$

故 $\varphi[k(y)h(y)]$ 之 x 的 i 次、y 的 j 次项系数恰好是

$$p_0(x)q_j(x) + p_1(x)q_{j-1}(x) + \cdots + p_j(x)q_0(x)$$

的 i 次项的系数,记为 c_{ij}.再令,

$$p_t(x) = a_{t0} + a_{t1}x + \cdots + a_{tn}x^n,$$
$$q_s(x) = b_{s0} + b_{s1}x + \cdots + b_{tn}x^n.$$

那么 $c_{ij} = \sum\limits_{t+s=j}\sum\limits_{p+q=i} a_{tp}b_{sq}$.

右端,

$$\varphi[k(y)] = \sum a_{tp}x^p y^t, \quad \varphi[h(y)] = \sum b_{sq}x^q y^s,$$

$\varphi[k(y)]\varphi[h(y)]$ 的 x 的 i 次项、y 的 j 次项系数亦为

$$\sum_{t+s=j}\sum_{p+q=i} a_{tp}b_{sq}.$$

所以,φ 是个同构映射. ▌

以上事实可轻而易举地在多文字多项式环 $F[x, y, z, \cdots]$ 中得到.

有了这些记号,对于环的子环的表示也很方便.

设 S 是环 R 的一个有 1 的可换子环,T 是 R 的一个子集,对

S 上任意一个 m 元多项式 $f(x_1,\cdots,x_m)$，用 T 的元素 $t_1,\cdots,t_m$ 代进去，就得到

$$f(t_1,\cdots,t_m)\in R.$$

令 $S[T]$ 表示取尽所有 S 上一元多项式、二元多项式……取尽 T 中任意有限个元素代入这些多项式，得到的 R 的元素的集合，即

$$S[T]=\{f(t_1,\cdots,t_m)\mid f(x_1,\cdots,x_m)\in F[x_1,\cdots,x_m],$$
$$m=1,2,\cdots;\ t_1,\cdots,t_m\in T\}.$$

命题 9 设 R 是个环，S 是 R 的有 1 可交换的子环，T 是 R 的一个子集. 则 $S\cup T$ 在 R 中生成的子环恰好是 $S[T]$.

证明 先证 $S[T]$ 是个子环. 设

$$f(a_1,\cdots,a_m),\quad g(b_1,\cdots,b_n)\in S[T].$$

$f(x_1,\cdots,x_m)\in F[x_1,\cdots,x_m]$，$g(y_1,\cdots,y_n)\in F[y_1,\cdots,y_n]$，那么 $f(x_1,\cdots,x_m)+g(y_1,\cdots,y_n)$ 是 F 上 $m+n$ 元多项式，$f(x_1,\cdots,x_m)g(y_1,\cdots,y_n)$ 也是 F 上 $m+n$ 元多项式. 从而

$$f(a_1,\cdots,a_m)g(b_1,\cdots,b_n)\in S[T],$$
$$f(a_1,\cdots,a_m)+g(b_1,\cdots,b_n)\in S[T].$$

$S[T]$ 为 R 的一个子环.

显然，$S\subseteq S[T]$，$T\subseteq S[T]$.

另一方面，R 的任意子环 K，若 $S\cup T\subseteq K$，那么，对 S 上任意一个 n 元多项式 $f(x_1,\cdots,x_n)$ 及任取 $a_1,\cdots,a_n\in T$，都必有

$$f(a_1,\cdots,a_n)\in K.$$

所以 $S(T)\subseteq K$.

这就说明了，$S[T]$ 是 $S\cup T$ 在 R 中生成的子环. ▌

实际上，定义交换环 S 上的多项式环 $S[x]$ 时，可以不要求 S 有恒等元，上述命题对 S 不含恒等元时也可以照搬过去.

本节最后，我们看域 F 上的 n 元多项式环 $F[x_1,\cdots,x_n]$. 由于 $F[x_1]$ 是有 1 可换的无零因子环，$F[x_1][x_2]$ 也是有 1 可换的

无零因子环……. $F[x_1,\cdots,x_n]\cong F[x_1][x_2]\cdots[x_n]$也是如此.

于是，由§3知，$F[x_1,\cdots,x_n]$有分式域. 我们暂时记为$F\{x_1,\cdots,x_n\}$. 到第七章时再赋予它新的记法.

$$F\{x_1,\cdots,x_n\}=\left\{\frac{f(x_1,\cdots,x_n)}{g(x_1,\cdots,x_n)}\;\middle|\; f,g\in F[x_1,\cdots,x_n],\ g\neq 0\right\}.$$

它的运算是

$$\frac{f(x_1,\cdots,x_n)}{g(x_1,\cdots,x_n)}+\frac{k(x_1,\cdots,x_n)}{h(x_1,\cdots,x_n)}=\frac{fh+gk}{g(x_1,\cdots,x_n)h(x_1,\cdots,x_n)},$$

$$\frac{f(x_1,\cdots,x_n)}{g(x_1,\cdots,x_n)}\cdot\frac{k(x_1,\cdots,x_n)}{h(x_1,\cdots,x_n)}=\frac{f(x_1,\cdots,x_n)k(x_1,\cdots,x_n)}{g(x_1,\cdots,x_n)h(x_1,\cdots,x_n)}.$$

与大家熟悉的数域上的有理函数的运算是一致的.

习　题　四

1. 设 R 是个有1的交换环，S 是 R 的子环，I 是 R 的理想. 证明：$S[x]$是 $R[x]$的子环，$I[x]$是 $R[x]$的理想.

2. 设 R 是个有1的交换环，K 是多项式环 $R[x]$的一个理想. 令

$$H=\{a\in R\mid a \text{ 是 } K \text{ 中某 3 次多项式之首系数}\}.$$

证明：$I=H\cup\{0\}$是 R 的一个理想.

3. 在 $\mathbf{Z}_6[x]$中求$(3^*x+2^*)(2^*x+5^*)$, $(3^*x+3^*)(4^*x^2+2)$, $(x+1^*)(x+2^*)$, $(x+4^*)(x+5^*)$.

4. 在环 $\mathbf{Z}_4[x]$中，1次多项式 2^*x+1^* 能不能是单位?

5. 设 F 是个域，$f(x)\in F[x]$，$c\in F$. 那么 $f(x)-f(c)\in(x-c)$，$(x-c)$是 $x-c$ 在 $F[x]$中生成的主理想.

6. 设 F 是个域，令任意

$$f(x)=a_0+a_1x+\cdots+a_nx^n$$

对应多项式

$$\bar{f}(x)=a_0+a_1x^2+\cdots+a_nx^{2n},$$

证明：环 $F[x]$到 $F[x]$的映射

$$\sigma: f\to\bar{f},\quad f\in F[x]$$

是环同态映射.

7. 设 σ 是环 R 到环 S 的同态映射. 证明:

$$\varphi: a_0 + a_1 x + \cdots + a_n x^n \to \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n$$

是环 $R[x]$ 到环 $S[x]$ 的同态映射, 给出 $\mathrm{Ker}(\varphi)$.

§5 素　　域

这一节,我们对域的子域做初步讨论,为第七章研究域的扩张问题做些准备.

定义 1 设 $(F,+,\cdot)$ 是个域. F 的子集 S 称为 $(F,+,\cdot)$ 的**子域**,如果

(1) $(S,+,\cdot)$ 是 $(F,+,\cdot)$ 的子环,

(2) $(S,+,\cdot)$ 本身是个域.

命题 1 设 S 是 F 的一个子环,且至少含 2 个元素. 那么, S 是 F 的子域,当而且仅当, $s\in S$, $s\neq 0$ 蕴涵 $s^{-1}\in S$. 其中 s^{-1} 代表元素 s 在域 F 中的逆元素.

证明 若 S 是 $(F,+,\cdot)$ 的子域,那么环 $(S,+,\cdot)$ 本身是个域. 设 e 是它的恒等元,对任意 $s\in S$, $s\neq 0$,用 $\bar{s}$ 代表 s 在 S 中的逆元. 用 1 代表 F 的恒等元. 从而有 $e\neq 0$,且

$e=e\cdot e$,　　　　(在 S 中,也在 F 中)

$e=1\cdot e$,　　　　(在 F 中)

$e=1$.　　　　　(在 F 中有消去律)

这就是说, S 的恒等元就是 F 的恒等元.

进一步,由

$\bar{s}s=e=1$,　　　　($\bar{s}$ 是 s 在 S 中的逆)

$s^{-1}s=1$,　　　　(s^{-1} 是 s 在 F 中的逆)

$s^{-1}=\bar{s}$,　　　　(消去非 0 元 s)

即 s^{-1} 就是 s 在 S 中的逆,当然有 $s^{-1}\in S$.

反过来,设 $(S,+,\cdot)$ 是 $(F,+,\cdot)$ 的一个子环,至少含 2 个元素. 且 $s\neq 0$, $s\in S$ 时 $s^{-1}\in S$. 那么我们取 $x\neq 0$, $x\in S$(这是能办

到的，因 S 至少含 2 个元素），由假定可知，$x^{-1}\in S$. 但 S 是 $(F, +, \cdot)$ 的子环，S 对 F 的乘法·封闭，故

$$1 = xx^{-1}\in S,$$

即 S 含 F 的恒等元 1，1 是 S 的恒等元.

又，对任意 $s\neq 0$，$s\in S$，由假定知 s^{-1} 也是 S 的元素，且

$$ss^{-1}=1,$$

s^{-1} 就是 s 在 S 中的逆元. $(S, +, \cdot)$ 是个域. ▌

推论 如果 S 是域 F 的子域，那么它们的恒等元相同. ▌

命题 2 设 F 是个域，T 是 F 的某些子域做成的集合，

$$T=\{S_a \mid S_a \text{ 是 } F \text{ 的子域}, a\in\Gamma\}.$$

那么这些子域的交集 $S=\bigcap_{a\in\Gamma} S_a$ 也是 F 的子域.

证明 这几乎就是环论中"若干个子环之交集仍为子环"的推论（见第四章 §2 命题 4）. 但是，要注意，域必须含两个以上元素. 因为，对任意 $a\in\Gamma$，S_a 都是 F 的子域，它必含有 F 的零元素 0 和恒等元素 1，所以，它们的交集 S 也必含有 0 和 1，S 至少含两个元素.

任意 $s\in S$，$s\neq 0$，那么 $s\in S_a$，对任意 $a\in\Gamma$ 都成立. 但 S_a 是个域，从而 $S^{-1}\in S_a$，$a\in\Gamma$. 于是 s^{-1} 就属于这些 S_a 的交集 S.

S 是 F 的一个子域. ▌

定义 2 设 F 是个域，T 是 F 的一个非空子集，F 的所有包含 T 的子域的交集称为是 T 生成的**子域**. 特别地，由 F 的零元素 0 和恒等元素 1 生成的子域称为 F 的**素域**.

例如，在实数域 $\mathbf{R}$ 中，所有有理数的集合 $\mathbf{Q}$ 所生成的 $\mathbf{R}$ 的子域就是 $\mathbf{Q}$，因为 $\mathbf{Q}$ 本身是个域，所有包含 $\mathbf{Q}$ 的子域（其中也有 $\mathbf{Q}$）的交就是 $\mathbf{Q}$.

所有正有理数的集合生成的子域也是 $\mathbf{Q}$. 因为一个子域必含有 0 且含某一正数时必含该数的相反数.

所有正整数的集合 $\mathbf{I}$ 生成的子域也是 $\mathbf{Q}$. 因为一个含 $\mathbf{I}$ 的子

域，首先必含 0 和 1，进而要含所有负整数，最后导致它必含每个有理数

$$\frac{a}{b},\quad a,b\in\mathbf{I},\ b\neq 0,$$

即该子域必含 $\mathbf{Q}$.

集合 $\{5\}$ 在 $\mathbf{R}$ 中生成的子域也是 $\mathbf{Q}$. 因为任何含 5 的子域必有 0 和 1，减法封闭，它必含

$$0-1=-1,\ 0-1-1=-2,\ \cdots,$$
$$1+1=2,\ 1+1+1=3,\ \cdots$$

即含所有整数，于是它必包含所有有理数.

集合 $\{\sqrt{5}\}$ 在 $\mathbf{R}$ 中生成的子域必包含所有有理数，从而包含所有形如

$$a+b\sqrt{5},\quad a,b\in\mathbf{Q}\qquad (*)$$

的实数. 而形如(*)的任意两数之差、之积仍有(*)形式，非零的形如(*)的数的倒数仍形如(*)，它们形成 $\mathbf{R}$ 的一个子域，就是 $\{\sqrt{5}\}$ 生成的子域.

定理 1 设 $(F,+,\cdot)$ 是个域. 那么，F 的素域 P 或者同构于有理数域或者同构于 $\mathbf{I}_p$，其中 p 是个素数.

证明 为了避免和有理数 1,0 混淆，将 F 的恒等元和零元分别记为 e 和 θ.

由于 $e\in P$，P 在减法之下封闭，必有

$$e+e=2e\in S,\quad (-2)e=(-e)+(-e)\in S.$$

进而对任意 $n\in\mathbf{I}$，ne 或为 n 个 e 相加，或为 $(-n)$ 个 $-e$ 相加 ($n<0$ 时)，同时 $\theta\in P$，故

$$ne\in P,\quad 对任意\ n\in\mathbf{I}.$$

建立整数环 $\mathbf{I}$ 到 F 的映射 φ,

$$\varphi: n\rightarrow ne,\quad n\in\mathbf{I}.$$

显然，这是加群 $(\mathbf{I},+)$ 到 $(F,+)$ 的群同态映射.

进一步，对任意 $m,n\in\mathbf{I}$，还有

$$\begin{aligned}
\varphi(mn)&=(mn)e &&(\varphi\text{ 的定义})\\
&=m(ne) &&(\text{加群中元素的乘幂})\\
&=mene &&(\text{第四章}\,\S1\text{ 命题 3})\\
&=\varphi(m)\varphi(n), &&(\varphi\text{ 的定义})
\end{aligned}$$

也就是说 φ 为 $\mathbf{I}$ 到 F 的环同态映射.

映射 φ 的像 $\mathrm{Img}(\varphi)$是 F 的子环,映射 φ 的核 $\mathrm{Ker}(\varphi)$是环 $\mathbf{I}$ 的理想. 在第四章 §2 已经证明了,$\mathbf{I}$ 的理想必为一主理想,从而 $\mathrm{Ker}(\varphi)$是由某个非负整数 m 生成的,即 $\mathrm{Ker}(\varphi)=(m)$.

φ 是 $\mathbf{I}$ 到 $\mathrm{Img}(\varphi)$上的满同态,由环同态基本定理,得

$$\mathbf{I}/(m)\cong\mathrm{Img}(\varphi).$$

当 $m=0$ 时,$\mathrm{Img}(\varphi)\cong\mathbf{I}$.

当 $m\neq0$ 时,因为

$$\mathbf{I}/(m)\cong\mathbf{I}_m=\{0^*,1^*,\cdots,(m-1)^*\}$$

而 $\mathbf{I}/(m)$同构于域 F 的子环,它不能含非零的零因子. 而第四章 §1 例题 4 已指明,$\mathbf{I}_m$ 不含非零的零因子,当而且仅当,m 为素数. 也就是说 $m\neq0$ 时必为素数. 据 §1 之例题 1, $\mathbf{I}_m$ 必为域. 此时,由

$$\mathbf{I}_m\cong\mathbf{I}/(m)\cong\mathrm{Ker}(\varphi)$$

知 $\mathrm{Ker}(\varphi)$是 F 的一个子域.

由于 P 是 F 的素域,它是 F 的所有子域的交集,故

$$P\subseteq\mathrm{Img}(\varphi).$$

同时,P 作为加法群,它是$(\mathrm{Img}(\varphi),+)$的子群. 由拉格朗日定理,$P$ 的元数 p 要整除 $\mathrm{Img}(\varphi)$的元数 m. 但 P 至少含 2 个元素,$p>1$,而 m 为素数,所以 $p=m$. $\mathrm{Img}(\varphi)=P$.

这样,对 $m\neq0$ 的情形,我们得到了所要的结论.

再回过头来看 $m=0$ 情形. 此时 $\mathrm{Img}(\varphi)\cong\mathbf{I}$,它们都是整环,由本章 §3 之命题 3 知,$\mathbf{I}$ 的分式环 $\mathbf{Q}$ 同构于 $\mathrm{Img}(\varphi)$的分式环 H.

任何域均含 e，从而，对任意 $n \in \mathbf{I}$，$ne = \varphi(n) \in P$，故 $\mathrm{Img}(\varphi) \subseteq P$. 再由 § 3 之例题 1 知，$P$ 必含一个子域 H' 同构子 H. 但是，P 不含任何不同于它的子域，否则与它定义相矛盾. 所以，$H' = P$. 从而

$$P = H' \cong H \cong \mathbf{Q}. \qquad \blacksquare$$

推论 域 F 的素域同构于 $\mathbf{I}_p$ 的充要条件是它的特征数为 p；F 的素域同构于 $\mathbf{Q}$ 的充分必要条件是 F 的特征数为 0.

事实上，定理之证明中，$\mathrm{Ker}(\varphi) = (p)$，即 $pe = 0$，从而对任意 $x \in F$ 都有

$$px = p(ex) = (pe)x = 0.$$

而对任意 $0 < n < p$，有 $ne \neq \theta$. 这说明 F 之特征数为 p. 反之亦然.

而 $\mathrm{Ker}(\varphi) = (0) = \{0\}$，即对任意 $n \in \mathbf{I}$，都有 $ne \neq \theta$，故特征数为 0. 反之，若特征数为 0，那么对任意 $n \in \mathbf{I}$ 必有 $x \in F$，$nx \neq 0$. 于是

$$nx = nex \neq \theta, \quad ne \neq \theta.$$

进而 $\mathrm{Ker}(\varphi) = \{0\}$. $\blacksquare$

推论 设 F 是个域，P 是它的素域. 那么 F 的任意子集 T 在 F 中生成的子域与 $T \cup P$ 生成的子域恒相等.

事实上，T 生成的子域必包含素域 P，从而包含 $T \cup P$ 生成的子域. 反过来则是十分明显的. $\blacksquare$

由于域的每个子域都含这个素域 P，所以也称素域为域的**最小子域**.

例题 1 设域 F 的特征数为 p. 那么集

$$S = \{\alpha \in F \mid \alpha^{p^n} - \alpha = 0,\ 0 < n \in \mathbf{I}\}$$

是 F 的一个子域.

证明 首先，$1^p - 1 = 0$ 和 $0^p - 0 = 0$ 表明 S 含有 F 的 0 和 1，S 至少含 2 个元素.

其次，任取 $\alpha, \beta \in S$，设

$$\alpha^{p^n}-\alpha=0,\ \beta^{p^m}-\beta=0,\ \alpha^{p^n}=\alpha,\ \beta^{p^m}=\beta,$$

其中 m,n 均为正整数.于是

$$\alpha^{p^{mn}}=\alpha^{p^n p^n\cdots p^n}=(\alpha^{p^n})^{p^{n(m-1)}}=\alpha^{p^{n(m-1)}}=\alpha,$$

$$\beta^{p^{mn}}=\beta^{p^m p^m\cdots p^m}=(\beta^{p^m})^{p^{m(n-1)}}=\beta^{p^{m(n-1)}}=\beta.$$

而且,F 之特征数为 p,由§1,

$$(\alpha-\beta)^{p^{mn}}=\alpha^{p^{mn}}-\beta^{p^{mn}}=\alpha-\beta,$$

即 $\alpha-\beta\in S$.同时,还有

$$(\alpha\beta)^{p^{mn}}=\alpha^{p^{mn}}\cdot\beta^{p^{mn}}=\alpha\beta,$$

也就是说 S 是 F 的子环.

最后,若 $\alpha\in S$, $\alpha\neq 0$,那么,由

$$\alpha^{p^n}-\alpha=0,\quad \alpha^{p^n}=\alpha,$$

知道 $\alpha^{-1}=(\alpha^{p^n})^{-1}=(\alpha^{-1})^{p^n}$, $\alpha^{-1}\in S$.

所以,S 是 F 的一个子域. ▌

习 题 五

1. 设 $(F,+,\cdot)$ 是个域.那么群 $(F,+)$ 的每个非零元素的周期(加法)都相同.

2. 设 F 是个域,其特征数为 p.那么 F 的每个子域的特征数均为 p.

若 S 是环 R 的子环,那么 S 的特征数与 R 的特征数一定相同吗?

3. 设 P 是域 F 的素域.那么对于 F 的每个自同构 σ 及任意 $x\in P$ 恒有

$$\sigma(x)=x.$$

小 结

域是一种特殊的环.关于域的理论研究的内容十分丰富,形成代数学中很多独立分枝,如伽罗华(Galois)理论、代数数论等.

环的某个同态像能否是个域?这是前一章关于环的理想与同

态的讨论的继续，没有什么新思想．但却由此引出了两个重要概念：素理想和极大理想．读者应通过大量的实例弄懂它们的共性与区别．不要因为整数环的极大理想与素理想是一致的而误认为在任何环中它们都是相同的．

关于"分式域"，有些验算工作是十分简单的，可以一带而过．我们同样要引起重视的是，这种用等价类方法进行的扩张思想．它使你认清整数环与有理数环本质联系．这种办法在其他领域也有广泛应用．

这一章的很大篇幅是讨论交换环上的多项式．希望读者一开始先抛开以往在初等数学或函数论中对多项式的意义，按这里的代数的定义先搞懂多项式、项、系数、次数、加法、乘法的定义．特别重要的是必须弄明白怎样的两个多项式是相等的．

由于交换环是各式各样的，所以在一个交换环上所有多项式构成的环可能有零因子，非常数多项式可能是单位，一个次数很低的多项式却可能有很多根（甚至无穷多个根）．这些现象都应引起足够重视，要仔细分析书中各例题，注意产生这些现象的原因．如果读者能自力更生构造一批例子来说明上述现象，那是最好不过的了．

对于域上的多项式，由于可用长除法，在处理多项式的次数、求根等方面都有极方面的条件．书中给出的定理和命题都是最基本的，在后两章中还要不断地用到．

一般域上的多项式与我们熟悉的有理数域、实数域上的多项式有相当多的本质上的相似之处．学这一段的时候要立足于"求同"，而学一般环上多项式的时候，则应比照数环"求异"．

多个文字多项式写起来比较复杂，按《自学考试大纲》不应讲述太多，这里提到的一些事实主要是为第七章作准备的．主要目的是帮助读者理解一个环或域再添上有限个元素后生成的环或域的结构．要求大家对本书后面提到的元素表达形式能够理解就行，不做深入要求．

复 习 题

1. 设 R 是个交换环，对 R 的任意一个理想 I，令

$$P(I)=\{x\in R\mid x^n\in I \text{ 对某个正整数 } n\}.$$

证明：$P(I)$是个理想；$P(I^2)=P(I)$；当 I 为素理想时 $P(I)=I$.

2. 设 R 是个有 1 的交换环. 证明：环 R 与环 $R[x]$的特征数相同.

3. 设 R 是个有 1 的交换环，对任意

$$f(x)=a_nx^n+\cdots+a_1x_1+a_0\in R[x],$$

规定 $\sigma:f(x)\to a_0$. 证明：σ 是 $R[x]$到 R 的环同态；求 $\mathrm{Ker}(\sigma)$和商环

$$R[x]/\mathrm{Ker}(\sigma).$$

4. 在 $\mathbf{I}_3[x]$中计算 $x(x-1^*)(x+1^*)(x^2+1)(x^2+x-1^*)(x^2-x-1^*)$.

5. 在域 F 上多项式环中，若 $f(x),g(x)\in F[x]$且它们生成的主理想相同$(f(x))=(g(x))$，那么它们的次数相等，$\deg f(x)=\deg g(x)$.

6*. 设 F 是个域，e 是它的恒等元. 任取 $a,b\in F$, $a\neq 0$. 构造一个 F 上的变换

$$\sigma_{a,b}:x\to ax+b,\quad \text{对每个 } x\in F.$$

证明：所有这种形式的变换

$$G=\{\sigma_{a,b}\mid a,b\in F,\ a\neq 0\}$$

是 F 上变换群的一个子群. 且

$$K=\{\sigma_{e,b}\mid b\in F\}$$

是 G 的一个正规子群. 给出商群 G/K 的结构.

7. 环 R 有 6 个元素，R 能不能是整环？

8. 有理数环 $\mathbf{Q}$ 上的 2 个文字的多项式环 $\mathbf{Q}[x,y]$中，x 生成的理想(x)是不是极大理想？

第六章　因子分解理论

学习初等代数时，人们常问，怎样的多项式的分解才算是彻底的分解呢？

有点数论知识的读者就会发现，多项式分解的过程与整数分解的过程颇有相似处．但它们最基本的相似之处何在呢？

本章，我们将整数、多项式及其他研究对象放到相应的环中进行研究，找出“因子分解”问题的最基本规律．所以，这里要讲的抽象的因子分解理论是整数和多项式分解理论的推广和深化．

学好这一章，会对初等数学中多项式因式分解和整数因子分解理论中含混不清之处从理论上有明确的认识．

同时，这一章的某些内容也是下一章域论的准备知识．

本章只讨论整环．

§1　整　　除

设 D 是个整环，e 是它的恒等元．

定义 1　设 $a,b\in D$，$b\neq 0$．说元素 b **能整除**元素 a，如果有 $c\in D$ 使得 $a=bc$．此时，也说 a 能被 b 整除，或说 b 是 a 的因子，并记为 $b\mid a$，否则，就说 b 不整除 a，记 $b\nmid a$．

在第四章§1，我们已经定义，某元素是 D 的单位，如果它能整除恒等元 e．某元素为单位的另一说法是它可逆，单位与单位元是不同的概念，单位元与恒等元是一回事．

例如，整数环 $\mathbf{I}$ 中，-1 和 1 均为单位，$1,-1,2,-2$ 均能整

除 2.

域中每个非零元均为单位.

$\mathbf{R}[x]$中多项式 $x-\sqrt{2}$整除 x^2-2.

例 1 设 F 是个域.那么 $f(x)$为 $F[x]$的一个单位的充要条件是 $f(x)=c\neq 0$.

这是因为,$f(x)g(x)=1$ 的充分必要条件是

$$\deg f(x)=0,\quad f(x)\neq 0.$$

而零次多项式就是非零常数多项式.

定义 2 设 $a,b\in D$.说元素 a 和元素 b 是**相伴的**,如果 $a|b$ 且 $b|a$.

命题 1 元素 a 和元素 b 是相伴的,必要而且只要,有 D 的单位 ε 使 $b=\varepsilon a$.

事实上,如果 a 和 b 是相伴的,$a|b$ 且 $b|a$,则必有 $c,d\in D$ 使

$$ac=b,\quad bd=a.$$

于是 $a=bd=acd$, $cd=e$. c 为单位.

反之,若 $b=\varepsilon a$, ε 为单位,则 ε 可逆,从而 $a=\varepsilon^{-1}b$,即 a 和 b 是相伴的. ∎

定义 3 对于 $a\in D$,所有单位及与 a 相伴的元素均称为 a 的**平凡因子**. a 的因子 b,不是其平凡因子者,称为**非平凡因子**.

D 的元素 a 不是单位也不是 0 且没有非平凡因子,则称 a 为**不可约元或既约元**.

例 2 整数环 $\mathbf{I}$ 中,素数 p 的因子只有 $1,-1,p$ 和 $-p$,故 p 是整数环 $\mathbf{I}$ 的不可约元.

例 3 域 F 上的多项式 $x-c$, $c\in F$,是环 $F[x]$的一个不可约元.

首先,$x-c$ 不是零多项式,也不是 $F[x]$的恒等元 1.

其次,若有 $f(x)\in F[x]$是 $x-c$ 的因子,设

$$f(x)g(x)=x-c,$$

则 $\deg f(x)$或为 1 或为 0.

当 $\deg f(x)=0$ 时,$\deg g(x)=1$. $f(x)$不能是零多项式,它只能是个非零常数,即 $f(x)$为环 $F[x]$的单位.

当 $\deg f(x)=1$ 时,$g(x)$只能是非零常数,即 $g(x)$是 $F[x]$的单位,$f(x)$与 $x-c$ 是相伴的.

总之,$x-c$ 没有非平凡因子.

例 4 看 $\mathbf{R}[x]$,$\mathbf{I}[x]$中的多项式 x^2-2.

在 $\mathbf{R}$ 上,因为

$$x^2-2=(x+\sqrt{2})(x-\sqrt{2}).$$

而 $x+\sqrt{2}$既不是 $\mathbf{R}[x]$中单元又不是与 x^2-2 相伴的,$x+\sqrt{2}$是 x^2-2 的非平凡因子. x^2-2 不是 $\mathbf{R}[x]$的不可约元.

在 $\mathbf{I}$ 上,若有整数 m,n,k,l 使

$$x^2-2=(mx+n)(kx+l),$$

则必有

$$x^2-2=mkx^2+(kn+ml)x+nl.$$

由多项式相等之定义,推出

$$mk=1,\quad -nl=2,\quad kn+ml=0,$$

从而 $m=k=\pm 1$. 这样,就导致

$$kn+ml=k(n+l)=0,$$

$$n+l=0,\quad -nl=2,$$

必有 $n^2=2$. 这是办不到的. 所以,x^2-2 在 $\mathbf{I}[x]$上不能有一次多项式作为其因子.

设 $x^2-2=f(x)g(x)$,则 $f(x)$或 $g(x)$必有一个次数为 0,为非零常数,也就是 $\mathbf{I}[x]$的单位,另一个必然是和 x^2-2 相伴的.

这说明 x^2-2 在 $\mathbf{I}[x]$中是不可约元.

命题 2 若 p 是D 的不可约元,ε 是D 的单位,则 εp 亦为D 的不可约元.

证明 首先,因为 D 为整环. 由 $p\neq 0$ 及 $\varepsilon\neq 0$ 知 $\varepsilon p\neq 0$.

其次,εp 必不是D 中单位. 若不然,就有 $a\in D$ 使得 $a(\varepsilon p)=$

$(a\varepsilon)p=e$,推出 p 为单位而导出矛盾.

最后,设 b 是 εp 的一个因子,有 $c\in D$ 使

$$\varepsilon p=bc.$$

由于 ε 是单位,有逆,故 $p=(\varepsilon^{-1}b)c$. 而 p 是不可约元,$\varepsilon^{-1}b$ 只能是单位,或者它是与 p 相伴的. 当 $\varepsilon^{-1}b$ 是单位时,b 必为单位;当 $\varepsilon^{-1}b$ 与 p 相伴时,有单位 $\delta\in D$ 使

$$\delta\varepsilon^{-1}b=p,$$

$\delta\varepsilon^{-1}$ 仍为单位,b 是与 p 相伴的. 这说明 b 一定是 p 的一个平凡因子.

即 εp 无非平凡因子,εp 是不可约元. ▌

命题 3 设 D 中元 a 非零,且

$$a=bc,\quad b,c\in D.$$

那么 b 为 a 的非平凡因子的充分必要条件是 c 为 a 的非平凡因子.

证明 如果 c 为 a 的平凡因子. 当 c 为单位时,b 是和 a 相伴的;当 c 是和 a 相伴的元素时,$c=\varepsilon a$, ε 为单位,于是

$$a=bc=\varepsilon ba,$$

而 $a\neq 0$, D 无非零的零因子,故 $\varepsilon b=e$, b 是单位. 也就是说,c 是平凡因子时,b 亦是平凡因子. ▌

定义 4 满足下列条件的整环 D 称为**唯一分解整环**:

(1) 如果 $a\in D$, $a\neq 0$, a 不是单位,那么 a 必可以写成若干个 D 的不可约元的乘积,即

$$a=p_1p_2\cdots p_s,\quad p_i \text{ 是 } D \text{ 的不可约元}.$$

(2) 如果 $a\in D$,且

$$a=p_1p_2\cdots p_s=q_1\cdots q_t,$$

其中 p_i 和 q_j 都是 D 的不可约元,那么 $s=t$,并且适当调整 q_j 的顺序后,可使 q_j 与 p_j 恰好是对应相伴的,$j=1,2,\cdots,t$.

这个定义之条件(1)对单位和零元不作要求,这是很自然的,因为在任何整环中,若

$$0=a_1a_2\cdots a_r$$

则必有 i 使 $a_i=0$，故 a_j 不能都是不可约元.

同样，若 ε 为 D 的单位，且

$$\varepsilon=a_1a_2\cdots a_r,$$

则每个 a_j 都是单位，都不是不可约元.

例如，整数环是唯一分解整环，每个非 0 又不为 1 或 −1 的整数 m，均有

$$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s},$$

其中 p_i 为素数，$\alpha_i\geqslant 1$. 而且，如果不计顺序，上述分解表达式是唯一的(可以差正负号).

又如，实多项式环 $\mathbf{R}[x]$ 是个唯一分解整环. 当实多项式 $f(x)$ 为非零非单位，即不是常数多项式时，必有

$$f(x)=p_1(x)^{\alpha_1}\cdots p_t(x)^{\alpha_t},\quad \alpha_i\geqslant 1, \tag{1}$$

其中每个 $p_i(x)$ 都是实的不可约多项式. 实数域上不可约多项式必为一次式或二次多项式.

这种分解，如果不计因式顺序，是唯一的(相应因式可相异一非零常数倍).

而复数域上多项式环 $\mathbf{C}[x]$ 的不可约元即不可约多项式必为一次式，每个非常数多项式 $f(x)$ 亦能表成以上(1)的形式，只不过诸 $p_i(x)$ 均为一次多项式. $\mathbf{C}[x]$ 也是唯一分解整环.

例 5 看复数环 $\mathbf{C}$ 的子环

$$\langle \mathbf{I}\cup\{\sqrt{-5}\}\rangle=\{a+b\sqrt{-5}\mid a,b\in\mathbf{I}\}.$$

它含 1，故为整环，亦记为 D.

为说明它不是唯一分解整环，建立映射

$$\varphi: a+b\sqrt{-5}\to a^2+5b^2,$$

这是 D 到整数环 $\mathbf{I}$ 的一个映射，即规定每个元素对应自己的模数的平方.

可以看出，对任意 $z,w\in D$，有

(1)　$\varphi(z)\geqslant 0$,

(2)　$\varphi(z)=0$ 当而且仅当 $z=0$,

(3)　$\varphi(zw)=\varphi(z)\varphi(w)$.

我们仅验证一下条件(3),设

$$z=a+b\sqrt{-5},\quad w=c+d\sqrt{-5},$$

其中 a,b,c,d 均为整数. 于是

$$\varphi(z)=a^2+5b^2,\quad \varphi(w)=c^2+5d^2.$$

再由 $zw=(a+b\sqrt{-5})(c+d\sqrt{-5})=ac+(-5bd)+(ad+bc)\sqrt{-5}$得

$$\begin{aligned}\varphi(zw)&=(ac-5bd)^2+5(ad+bc)^2\\&=(ac)^2+5(ad)^2+5(bc)^2+25(bd)^2\\&=(a^2+5b^2)(c^2+5d^2)\\&=\varphi(z)\varphi(w).\end{aligned}$$

现在来决定 D 中的单位. 若 $zw=1$,那么

$$\varphi(z)\varphi(w)=\varphi(1)=1.$$

而 $\varphi(z)$和 $\varphi(w)$都是整数,又非负,故

$$\varphi(z)=1,\quad \varphi(w)=1.$$

设 $z=a+b\sqrt{-5}$. 再由

$$\varphi(3)=1=a^2+5b^2,$$

知 $b=0,a=\pm 1$. 也就是说,D 中单位中有 1 和 -1.

D 中元素 x 仅仅与自己,与 $-x$ 是相伴的.

观察 $9=3\cdot 3=(2+\sqrt{-5})(2-\sqrt{-5})$,其中 $9,3,2+\sqrt{-5}$ 和 $2-\sqrt{-5}$都是 D 中元素,而 3 和 $2+\sqrt{-5}$、和 $2-\sqrt{-5}$都不是相伴的.

剩下来,我们只需证明 3 和 $2+\sqrt{-5}$都是 D 的不可约元. 设有 $z,w\in D$ 使 $3=zw$. 那么

$$\varphi(zw)=\varphi(3)=9=\varphi(z)\varphi(w).$$

$\varphi(z)$只能是 1,3 或者 9. 若 $\varphi(z)=1$,它是单位;若 $\varphi(z)=9$,则

$\varphi(w)=1$, w 是单位, z 与 3 是相伴的. 两种情形下, z 都不是整数 3 的非平凡因子.

要想使 3 有非平凡因子, 只能是

$$\varphi(z)=a^2+5b^2=3, \quad a, b \in \mathbf{I}.$$

但这是不可能的. 这说明 3 是整环 D 中的不可约元.

同样, 由于 $\varphi(2+\sqrt{-5})=9$, 若有 $z, w \in D$ 使 $zw=2+\sqrt{-5}$, 则必有

$$\varphi(z)\varphi(w)=\varphi(2+\sqrt{-5})=9.$$

$\varphi(z)$ 只能是 1 或 9, z 只能是单位或是与 $2+\sqrt{-5}$ 相伴的.

$2+\sqrt{-5}$ 和 $2-\sqrt{-5}$ 也是 D 的不可约元.

定理 1 设 D 是个唯一分解整环, p 是个不可约元. 如果 $p|(ab)$, 那么 $p|a$ 或 $p|b$.

证明 如果 $p|(ab)$, 设有 $c \in D$ 使 $ab=pc$.

当 a, b 均不为 0, 也不是 D 中单位时, c 必不为 0. 而且 c 也不能是单位, 否则, 必有

$$p=(c^{-1}a)b.$$

而 p 是素元, 上式导致 $c^{-1}a$ 为单位. 同时, 只要 $c^{-1}a$ 为单位则 a 亦为单位, 矛盾.

这样, 由于 c 不是 0 也不是单位, 而 D 是唯一分解整环, 必有

$$c=p_1p_2\cdots p_n,$$

其中每个 p_i 都是 D 的不可约元. 于是

$$ab=pp_1\cdots p_n,$$

就是元素 ab 的一个不可约因子分解式.

但 a, b 均不为 0 又不为单位, 它们可单独分解为

$$a=q_1q_2\cdots q_m, \quad b=r_1r_2\cdots r_t,$$

其中 q_j 和 r_k 也都是 D 的不可约元. 于是, 我们得到

$$ab=q_1\cdots q_mr_1\cdots r_t=pp_1p_2\cdots p_n,$$

据唯一分解整环的定义, 不可约元 $q_1, \cdots, q_m, r_1, \cdots, r_t$ 中必然有

一个与 p 是相伴的.

如果 q_j 是与 p 相伴的,由 $q_j|a$ 可推知 $p|a$;如果 r_k 是与 p 相伴的,由 $r_k|b$ 可推出 $p|b$.

当 $a=0$ 时,当然有 $p|a$. 即任意不可约元 p 都满足定理要求.

当 a 为单位时,$ab=cp$ 蕴涵 $b=(a^{-1}c)p$,也就是 $p|b$.

所以,当 a 和 b 有一个为 0 或有一个为单位时,定理恒对. ▌

定理 1 引起我们讨论另一个重要概念.

定义 5 设 D 是个整环,$p\in D$. 若 p 不是零元也不是单位,且对任意 $a,b\in D$,只要 $p|(ab)$,那么必有 $p|a$ 或者 $p|b$,则说 p 是 D 的一个**素元**.

从定义中可以看出,对任意整环 D 来说,它的素元 p 一定是不可约的. 因为,若

$$p=ab,\quad a,b\in D,$$

当然有 $p|(ab)$,由 p 的素性,必有 $p|a$ 或 $p|b$. 如果 $p|a$,则 a 与 p 是相伴的,b 为单位;如果 $p|b$,则 b 与 p 是相伴的,a 为单位. 从而 p 不能有非平凡因子.

定理 1 指明,对于唯一分解整环,p 是不可约元则一定是素元.

那么,对于一般的一个整环,素元和不可约元是否是同一概念呢? 仔细研究上面的例 5 即可说明问题. 在整环 $D=\langle \mathbf{I}\cup\{\sqrt{-5}\}\rangle$ 中,3 是个不可约元,3 能整除 9,且

$$9=(2+\sqrt{-5})(2-\sqrt{-5}).$$

但 $2+\sqrt{-5}$ 和 $2-\sqrt{-5}$ 都是 D 的不可约元,且它们都不是和 3 相伴的,所以

$$3\nmid(2+\sqrt{-5}),\quad 3\nmid(2-\sqrt{-5}).$$

这说明 3 是不可约元但不是素元.

由于整数环和域上多项式环都是唯一分解整环,素元与不可

约元一致，人们也把素数称为不可约数，把不可约多项式称为素多项式.

我们在处理唯一分解整环的整除性问题时，对不可约元和素元就不必区别了.

定义 6 设 D 是个整环，$a_1,\cdots,a_n\in D$. 如果 $c\in D$，c 整除 $a_1,\cdots,a_n$ 的每一个，则说 c 是元素 $a_1,\cdots,a_n$ 的一个**公因子**.

元素 $d\in D$ 称为元素 $a_1,\cdots,a_n$ 的一个**最大公因子**，如果

(1) d 是 $a_1,\cdots,a_n$ 的一个公因子，

(2) 对任意 $c\in D$，只要 c 是 $a_1,\cdots,a_n$ 的一个公因子，则必有 $c\mid d$.

当一个单位是 $a_1,a_2,\cdots,a_n$ 的一个最大公因子时，则说它们**是互素的**.

定理 2 设 D 是唯一分解整环. 那么不全为 0 的元素 a,b 必有最大公因子. 且各最大公因子都是相伴的.

证明 当 $a=0$ 时，必有 $b\neq 0$，b 就是 a 和 b 的最大公因子；当 $b=0$ 时，a 就是 a,b 的最大公因子.

当 a 为单位时，a 就是 a,b 的最大公因子；当 b 为单位时，b 就是 a,b 的最大公因子.

故，不妨设 a 和 b 都不是 0，也都不是单位. 于是，可设

$$a=p_1p_2\cdots p_s,\quad b=q_1q_2\cdots q_t.$$

其中 p_i 和 q_j 都是 D 的素元. 我们先将 a 的诸因子 p_i 中相伴的元素合在一起，写成

$$a=\varepsilon p_1^{l_1}p_2^{l_2}\cdots p_n^{l_n},\quad l_i\geqslant 1.$$

ε 是单位. 再把 b 的诸因子 q_j 中与 $p_1,\cdots,p_n$ 相伴的合在一起，写在前面，其余因子列后，即

$$b=\delta p_1^{k_1}\cdots p_n^{k_n}q_1\cdots q_k,$$

其中 δ 是 D 中单位，$k_j\geqslant 0$（当 p_j 不是 b 的非平凡因子时，$k_j=0$），q_t 不是 a 的非平凡因子，与任意 p_i 都不是相伴的.

用 $\min\{k, l\}$ 代表自然数 k, l 之最小者，令

$$s_j = \min\{k_j, l_j\}, \quad 1 \leqslant j \leqslant n.$$

可以断言，$d = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$ 就是 a, b 的一个最大公因子.

显然，a 和 b 的表达式中都含因子 d. 即 d 是 a, b 的公因子.

进一步，设 c 是 a, b 的任意一个公因子. 若 c 是个单位，自然有 $c \mid d$. 若 c 不是单位，

$$c = r_1 \cdots r_m, \quad r_i \text{ 是素元},$$

那么，由 $c \mid a$，$r_i \mid a$ 知，每个 r_i 必然是与某个 p_i 相伴的，把相伴的元素合在一起

$$c = \rho p_1^{h_1} p_2^{h_2} \cdots p_n^{h_n}, \quad h_k \geqslant 0.$$

再由 $c \mid a$，即

$$a = \epsilon p_1^{l_1} \cdots p_n^{l_n} = f(\rho p_1^{h_1} p_2^{h_2} \cdots p_n^{h_n})$$

可知 $h_1 \leqslant l_1$，否则(即 $l_1 < h_1$)，用消去律，得

$$\epsilon p_2^{l_2} \cdots p_n^{l_n} = f \rho p_1^{h_1 - l_1} \cdots p_n^{h_n}, \quad h_1 - l_1 > 0,$$

必有 $p_1 \mid (p_2^{l_2} \cdots p_n^{l_n})$，与诸 p_i 之不相伴的假设相矛盾. 同理，$h_2 \leqslant l_2, \cdots, h_n \leqslant l_n$. 又同理，

$$h_1 \leqslant k_1, \quad h_2 \leqslant k_2, \quad \cdots, \quad h_n \leqslant k_n.$$

也就是 $h_i \leqslant s_i = \min\{l_i, k_i\}$，从而必有 $c \mid d$，d 是 a, b 的一个最大公因子.

设 d^* 也是 a, b 的一个最大公因子. 因为 d 是个公因子，故 $d \mid d^*$. 而我们已经证明了 d 是最大公因子，又必有 $d^* \mid d$，即 d^* 是和 d 相伴的.

每个最大公因子都是和 d 相伴的，从而它们都是相伴的. ▌

推论 设 D 是个唯一分解整环. 那么任意 n 个不全为 0 的元素 $a_1, a_2, \cdots, a_n$ 必有最大公因子. ▌

例题 1 设 D 是个唯一分解整环，a, b 不全是 0，d 是它们的一个最大公因子. 那么，对于 D 中任意非零元 c，cd 恰为 ac, bc 的一个最大公因子.

证明 读者可以试用定理 2 的证明中使用的方法,将 a,b,c 写成素元连乘积,然后求出 ac 和 bc 的最大公因子.

这里用另一种方法证明.由于 ca,cb 不全为 0,它们必有最大公因子,设 f 是它们的一个最大公因子.首先,d 是 a,b 的公因子,$d|a$, $d|b$,故

$$(cd)|(ca),\quad (cd)|(cb),$$

即 cd 是 ca 和 cb 的一个公因子.据 f 的定义,$(cd)|f$.

于是,可设有 $x\in D$, $f=cdx$.

其次,f 是 ac 的因子,又是 bc 的因子,必有 $r,s\in D$ 使

$$ac=fr,\quad bc=fs,$$

$$ac=cdxr,\quad bc=cdxs.$$

因为 c 不为 0,用消去律,得

$$a=dxr,\quad b=dxs.$$

这说明 dx 是 a 和 b 的公因子.由 d 的定义知,$(dx)|d$.从而 d 与 dx 是相伴的,x 是个单位.

最后,由 $f=cdx$ 知 f 和 cd 是相伴的. ▌

例题 2 设 D 是个整环,而且

(1) 如果 $a\in D$, $a\neq 0$, a 不是单位,那么,a 必可写成若干个 D 的不可约元的乘积,即

$$a=p_1p_2\cdots p_s,\quad p_i \text{ 是 } D \text{ 的不可约元}.$$

(2) 对于 D 的任意不可约元 p, $p(ab)$ 蕴涵 $p|a$ 或 $p|b$.

则 D 必为唯一分解整环.

分析 接着唯一分解整环定义要求,只需证明分解表达式的唯一性.设

$$a=p_1p_2\cdots p_s=q_1q_2\cdots q_t, \tag{*}$$

其中 p_i 和 q_i 都是不可约元,需证明 $s=t$,适当调整顺序后,p_i 是与 q_i 相伴的.

条件(2)表面上是 $p|(ab)$ 则 $p|a$ 或 $p|b$,实际上蕴涵着 $p|(a_1a_2\cdots a_n)$,则 p 必然整除 a_i 中的一个.

因此,我们可以对(*)式左端之 s 用数学归纳法.

证明 设在 D 中有不可约元 p_i, q_j, $i=1,\cdots,s$; $j=1,\cdots,t$ 使

$$p_1p_2\cdots p_s=q_1q_2\cdots q_t \tag{*}$$

成立.我们对 s 用数学归纳法来证明必有 $s=t$ 且调整顺序后 p_i 和 q_i 是相伴的,$i=1,2,\cdots,s$.

当 $s=1$ 时,

$$p_1=q_1\cdots q_t=q_1(q_2\cdots q_t),$$

由于 p_1 是素元,故 q_1 或为单位或是与 p_1 相伴的.但 q_1 也是不可约元,不为单位,所以 q_1 必然是与 p_1 相伴的.

p_1 和 q_1 是相伴的,如果 $t\geqslant 2$,那么 $q_2\cdots q_t$ 必为单位,而 $q_2\cdots q_t$ 都是不可约元,这是不可能的.从而只有 $s=t=1$ 才行.命题当 $s=1$ 时得证.

现假定命题对 $s-1$ 情形是对的.那么

$$p_1p_2\cdots p_s=q_1q_2\cdots q_t \tag{*}$$

意味着 p_1 必整除 $q_1,\cdots,q_t$ 之一,因为允许适当调整顺序,我们不妨假定 $p_1|q_1$.

由于 q_1 也是不可约元,p_1 又不是单位,从而 p_1 是与 q_1 相伴的.设 $q_1=\varepsilon p_1$,ε 是单位.于是(*)变成

$$p_1p_2\cdots p_s=p_1\varepsilon q_2\cdots q_t.$$

$p_1\neq 0$,可用消去律,得

$$p_2\cdots p_s=q_2'q_3\cdots q_t, \tag{**}$$

其中 $q_2'=\varepsilon q_2$ 仍然是不可约元.

注意,(**)式之左端为 $s-1$ 个不可约元之积,右端是若干个不可约元之积,按归纳法假定,必然有 $s-1=t-1$,即 $s=t$ 而且调整 q_j 的顺序后,p_2 和 q_2'是相伴的,p_3 是和 q_3 相伴的……p_s 是和 q_s 相伴的.

由于 q_2' 与 q_2 相伴，故 p_2 与 q_2 是相伴的. 归纳法完成. ▮

例题 3 研究有理数环 $\mathbf{Q}$ 的子集

$$R=\{a/b\in\mathbf{Q}\mid b\text{ 为奇数}\}.$$

(1) R 对有理数减法和乘法封闭，R 是 $\mathbf{Q}$ 的子环，$1=1/1\in R$. R 是个整环.

(2) 任取 $a/b\in R$，如果 $c/d\in R$ 使

$$(a/b)\cdot(c/d)=1,$$

即 $ac=bd$，由于 b 和 d 都是奇数，从而 a 必为奇数.

反过来，若 $a/b\in R$，a 为奇数，必有

$$(a/b)\cdot(b/a)=1,$$

即 a/b 是 R 的单位.

所以，R 中元素 a/b 为单位的充要条件是 a 为奇数.

(3) 如果有 $a/b, c/d\in R$ 使

$$(a/b)\cdot(c/d)=2=2/1,$$

则 $ac=2bd$，2 必整除 a 或整除 c. 若设 $a=2f$，那么由

$$fc=bd$$

可知 f 必为奇数，$a/b=2\cdot(f/b)$. 这说明 a/b 是和 2 相伴的. 若 2 整除 c，则 a 为奇数，a/b 必然是个单位.

所以，2 没有非平凡因子，2 是环 R 的一个不可约元.

(4) 任取 $a/b\in R$，若它不是 0 也不是单位. 即 a 不为 0 也不为奇数，可设 $a=2^t d$，d 是个奇数. 于是

$$a/b=(d/b\cdot 2)2\cdot\cdots\cdot 2,\quad t\text{ 个 }2,$$

其 $d/b\cdot 2$ 和 2 都是 R 的不可约元，a/b 已写成不可约元的连乘积形式.

(5) 任取 $a/b\in R$，如果 $4\mid a$，$a=4c$，那么

$$a/b=2\cdot(2c/b).$$

说明，2 是 a/b 的因子且不是和 a/b 相伴的，即 2 是 a/b 的非平凡因子. a/b 不是不可约元，这说明，a 为奇数时，a/b 是 R 的单位，$4\mid a$ 时，a/b 不是不可约元.

所以，R 的所有不可约元都是和 2 相伴的.

(6) 我们用 $\|$ 代表环 R 中的整除符号，以区别本题前面用的整数的整除符号 1.

设 $a/b, c/d \in R$，

$$2 \| \{(a/b)\cdot(c/d)\},$$

即有 $f/h \in R$，使 $(a/b)\cdot(c/d) = 2\cdot(f/h)$，也就是

$$2fbd = ach.$$

由于 h 是奇数，2 不能(整数的)整除 h，从而 $2|a$ 或 $2|c$. 即

$$2 \| (a/b) \text{或} 2 \| (c/d),$$

由上题可知 R 是唯一分解整环. ▌

本节最后，我们希望读者能自己仿照例题 1 来证明更一般的情形.

命题 4 设 D 是个唯一分解整环. $a_1, a_2, \cdots, a_n \in D$，不全为 0，$d$ 是它们的一个最大的公因子. 那么，对任意 $c \in D$，$c \neq 0$，元素 cd 恰为 $a_1c, a_2c, \cdots, a_nc$ 的一个最大公因子. ▌

习 题 一

1. 在整环 $I_5[x]$ 中找出所有单位，给出 $2^* x^3 + x$ 的所有相伴元.

2. 证明：在整环 $I_2[x]$ 中，$x^3 + x + 1^*$ 是不可约元.

3. 复数环 $\mathbf{C}$ 中由整数集 $\mathbf{I}$ 和 $\sqrt{-2}$ 生成的子环，记为 $\mathbf{I}[\sqrt{-2}]$. 问，5 在 $\mathbf{I}[\sqrt{-2}]$ 中是不是不可约元素.

4. 设 F 是个域，$a, b \in F$. 证明：在 $F[x]$ 中，$x-a$ 与 $x-b$ 互素的充分必要条件是 $a \neq b$.

5. 设 D 是个唯一分解整环，$a, b \in D$. 那么 a, b 互素的充分必要条件是它们不含相同的素元因子.

6. 设 D 是个整环，把元素之间的整除看成是 D 上的一个关系. 证明：如果整除关系在 D 的非零元素 $D^* = D - \{0\}$ 上是个等价关系，那么 D 必然是个域.

7. 设 x, y 是整环 D 的元素. 证明：

(a) $x|y$ 的充要条件是$(x)\supseteq(y)$;

(b) x 和 y 相伴的充分必要条件是$(x)=(y)$;

(c) y 是 x 的非平凡因子的充分必要条件是$(x)\subset(y)\subset D$.

§2 主理想整环和欧氏环

要像上节例题 2 那样给出更多的环为唯一分解整环的充分必要条件当然是很有意义的事情. 同时,为了应用方便,也需要得到一些环为唯一分解整环的充分条件,本节介绍其中两种.

定义 1 如果整环 D 的每个理想都是主理想,则说 D 是主理想整环.

例如,整数环 $\mathbf{I}$ 是个主理想整环.

第四章 §4 定理 2 证明了,域 F 上的多项式环 $F[x]$ 是个主理想整环.

例 1 看上节例题 3 中的

$$R=\{a/b\in\mathbf{Q}\mid b \text{ 为奇数}\}.$$

设 N 是 R 的一个理想. 当 $N=\{0\}$ 时 N 恰为零元 0 生成的主理想 (0).

当 $N\neq\{0\}$ 时. 对任意 $a/b\in N$,设

$$a/b=2^t(c/b),\quad c \text{ 为奇数},\ t\geqslant 0.$$

可以证明,非负整数 t 是由元素 a/b 完全确定的.

设 $a/b=e/f$,其中 b 和 f 都是奇数. 由 $af=be$ 及整数的唯一分解定理,e 和 a 必含相同个 2 的因子,都是 t 个. 故

$$e/f=2^t(h/f),$$

h 和 f 都是奇数. 这说明,t 与 a/b 表达中元素选择无关.

建立映射

$$\varphi: a/b\to t,\quad a/b=2^t(c/b),\quad c \text{ 为奇数}.$$

这是环 N 到整数环 $\mathbf{I}$ 的一个映射.

由于 $\mathrm{Img}(\varphi)$ 是个非负整数的集合,它必有最小元,设为 n. 既

然 $n\in \mathrm{Img}(\varphi)$,那么必有 R 的元素 g/d 使得

$$\varphi(g/d)=n,\quad g/d=2^n(l/d),\quad l \text{ 为奇数}. \qquad (*)$$

现在,我们任取 $a/b\in N$,由 n 的定义,必有

$$n=\varphi(g/d)\leqslant\varphi(a/b)=t,$$

其中 $a/b=2^t(c/b)$,c 是个奇数.故

$$a/b=2^t(c/b)=2^n(l/d)\cdot(d/l)\cdot 2^{t-n}(c/b),$$

其中 $t-n\geqslant 0$, $2^{t-n}(c/b)\in R$.从而 $2^n(l/d)=g/d$ 在 R 整除 a/b,即 $a/b\in(g/d)$, $N=(g/d)$.

这说明 R 的每个理想都是主理想.

命题 1 设 D 是个主理想整环.那么,在 D 中不能有这样无穷多个理想 $N_1,N_2,\cdots$,使

$$N_i\subseteq N_{i+1},\quad N_i\neq N_{i+1},\quad i=1,2,\cdots.$$

证明 用反证法.若有无穷多个理想 $N_i(i=1,2,\cdots)$使得 $N_i\subseteq N_{i+1}$,且 $N_i\neq N_{i+1}$,令 $N=\bigcup_i N_i$ 可以证明它亦为 D 的一个理想.

首先,对任意 $x,y\in N$,据并集 N 的定义,x,y 必分别属于某个 N_i 和 N_j,即

$$x\in N_i,\quad y\in N_j.$$

在 i 和 j 两个自然数中不妨设 $i\leqslant j$,于是由诸 N_i 前面包含关系知 $N_i\subseteq N_j$.从而,有

$$x\in N_i\subseteq N_j,\quad y\in N_j.$$

但是,已知 N_j 是 D 的理想,故 $x-y\in N_j$,进一步,$x-y\in N_j\subseteq N$. N 对减法封闭.

其次,对任意 $r\in D$, $x\in N$.设 $x\in N_i$,那么,由于 N_i 是 D 的理想,必有 $rx,xr\in N_i$.从而 $rx,xr\in N_i\subseteq N$.

所以,N 为 D 的一个理想.

D 为主理想环,设 $N=(x)$.可是,据 N 的定义,$x\in N$ 则 x 必属于某个 N_i.进而(x)的所有元素都应属于 N_i,对于这个 i,有

$$N_{i+1} \subseteq N-(x) \subseteq N_i \subseteq N_{i+1};$$

也就是 $N_i = N_{i+1}$. 与假定相矛盾. ▌

命题 2 设 D 是个主理想整环, $p \in D$, $p \neq 0$. 那么, 下列说法等价:

(1) p 是 D 的一个素元;

(2) (p) 是 D 的一个极大理想;

(3) (p) 是 D 的一个素理想.

证明 用循环证法. 如果 p 是 D 的素元, 那么 p 不是单位, 故

$$1 \notin (p) = \{rp \in D \mid r \in D\}.$$

所以, $(p) \neq D$.

设 N 是 D 的理想, $(p) \subseteq N$, $(p) \neq N$. 由于 D 是主理想环, 可设 $N = (a)$, $a \in D$. 于是, $p \in N$ 意味着有 $b \in D$ 使 $p = ab$.

又由于 p 是素元, a 必为单位或者是与 p 相伴的. 如果 a 是和 p 相伴的, 则必有 $a \in (p)$, 从而 $(a) = N = (p)$, 与假设矛盾. 故, a 只能是个单位, 而单位生成的理想就是 D 本身. 所以 $N = D$. (p) 是个极大理想.

这样, 我们由条件(1)推出了条件(2).

下面, 由(2)推(3). 设 (p) 是极大理想. 由第五章§2 知剩余环 $D/(p)$ 是个域, 任取 $a, b \in D$, 如果 $ab \in (p)$, 那么在 $D/(p)$ 中

$$ab + p = [a + (p)][b + (p)] = p,$$

其中 p 乃是 $D/(p)$ 的零元. 而域当然不含非零的零因子, 故 $a + (p) = (p)$ 或 $b + (p) = (p)$, 也就是 $a \in (p)$ 或 $b \in (p)$. (p) 是 D 的素理想.

最后, 由(3)来推(1). 设 (p) 是个素理想. 如果有 $a, b \in D$ 使 $ab = p$. 那么 $ab \in (p)$, 于是必有 $a \in (p)$ 或 $b \in (p)$.

若 $a \in (p)$, 则 $p \mid a$, 从而 a 是和 p 相伴的, b 为 D 的一个单位. 若 $b \in (p)$, 则 b 是与 p 相伴的, a 是 D 的一个单位. 总之, p 没有任何非平凡因子. 又因为 $(p) \neq D$, p 不是 D 的单位, 同时 $p \neq 0$, 故 p 为 D 之素元. ▌

定理 1 每个主理想整环 D 都是唯一分解整环.

证明 现先来证明当 D 为主理想整环时,它的非 0 非单位的元素必为若干素元之积.

若不然,设 $a\in D$, $a\neq 0$, a 不是单位,且 a 不能写成若干个素元之乘积.

那么,首先,a 必然不是素元,否则 $a=a$ 即为素元积形式.于是 a 必然仅有非平凡的因子,设 b 和 c 是 a 的非平凡因子,$a=bc$.于是

$$a\in(b),\quad a\in(c).$$

并且,由于 b 和 c 均不是和 a 相伴的,必有

$$b\notin(a),\quad c\notin(a).$$

从而,有

$$(a)\subseteq(b),(a)\neq(b),(a)\subseteq(c),(a)\neq(c).$$

其次,由 $a=bc$,而 a 不是素元连乘积,可以断言 b 或 c 必然至少有一个也不是素元连乘积(当 b 和 c 均为素元乘积时,$bc=a$ 就是素元之积),取这样一个不是素元乘积者记为 a_1,它满足

(1) a_1 是 a 的非平凡因子,$(a)\subseteq(a_1)$, $(a)\neq(a_1)$;

(2) a_1 不能写成素元之连乘积形式.

由(1)可知 a_1 非 0 非单位,由(2)进一步知道 a_1 具有和 a 完全一样的性质.

最后,我们完成仿照对 a 的讨论,可找到 $a_2\in D$, $(a_2)\subseteq(a_1)$, $(a_2)\neq(a_1)$且 a_2 不是素元之积.这样不断做下去,即有

$$(a)\subseteq(a_1)\subseteq\cdots,\quad (a_i)\neq(a_{i+1}),\quad i=1,2,\cdots.$$

而命题 1 已经证明了,在主理想整环里是不能有这种结论的.这表明对 a 的假定不能成立.

再来证明 D 有分解的唯一性.设

$$p_1p_2\cdots p_s=q_1q_2\cdots q_t,\tag{*}$$

其中 p_i 和 q_j 都是 D 的素元.p_1 是素元,由命题 2 知,(p_1)是 D 的

一个素理想.(*)表明,

$$q_1q_2\cdots q_t\in(p_1),$$

故必有某个 $q_l\in(p_1)$,因为顺序可以不考虑,我们不妨假设 $q_1\in(p_1)$,即 $p_1|q_1$.但 q_1 是素元,p_1 是 q_1 是因子,p_1 必然是与 q_1 相伴的.

$$p_1=\epsilon q_1,\quad \epsilon\text{ 是单位}.$$

将(*)中 p_1 消去,得

$$p_2\cdots p_s=(\epsilon q_2)\cdots q_t,$$

其中 ϵq_2 也是素元.

继续下去并不断调整右端素元顺序,即有 p_i 和 q_i 是相伴的,对所有 $i=1,2,\cdots,t$ 都成立,同时 $s=t$. ▎

例题 1 设 D 是个主理想整环,其元素 a,b 不全为 0.那么,必有 $m,n\in D$ 使得 $d=ma+nb$ 恰好是 a,b 的一个最大公因子.

证明 看 D 中由子集 $\{a,b\}$ 生成的理想 N.由于 D 有 1 且可交换,N 中每个元 r 必可写成

$$r=xa+yb,\quad x,y\in D.$$

另一方面,D 是主理想环,必有 $d\in D$ 使 $N=(d)$.设 $d=ma+nb$,我们来证明 d 是 a 和 b 的一个最大公因子.

首先,$a\in N=(d)$, $a=cd$, $d|a$.同样,$b\in(d)$, $d|b$.所以,d 是 a,b 的一个公因子.

其次,假设 f 是 a,b 的公因子,由 $f|a$ 和 $f|b$ 立知 $f|(ma+nb)$,即 $f|d$.

所以,d 是 a 和 b 的一个最大公因子. ▎

现在再介绍整环为唯一分解整环的另一个判别方法.

定义 2 整环 D 称为**欧氏环**,如果由 D 之所有非 0 元集合 D_0 到非负整数集 $\mathbf{I}_+$ 的映射 d 满足

(1) 如果 $a,b\in D_0$ 且 $a|b$,则 $d(a)\leqslant d(b)$;

(2) 如果 $a\in D$, $b\in D_0$,则必有 $q,r\in D$ 使 $a=bq+r$,

$d(r)<d(b)$或 $r=0$.

例如,整数环 **I** 上规定每个数对应其绝对值

$$d(r)=|r|,\quad r\in D$$

利用整数的长除法,即知 **I** 即为一个欧氏环.

又如,对任意域 F,规定

$$d: f(x)\to \deg f(x),\quad f(x)\in F[x],\quad f(x)\neq 0,$$

即得所有非 0 多项式集 $F[x]_0$ 到非负整数集 $\mathbf{I}_+$ 的一个映射.

在第五章§4 定理 1 中,我们证明了,对任意 $f(x)\in F[x]$, $g(x)\in F[x]_0$,必有 $q(x),r(x)\in F[x]$使得

$$f(x)=g(x)q(x)+r(x),\quad \deg r(x)<\deg g(x).$$

由于原来规定了零多项式的次数为 $-\infty$,那里的

$$\deg r(x)<\deg g(x)$$

就包含了两种情形,$r(x)$为 0,或者

$$0\leqslant \deg r(x)<\deg g(x).$$

这与欧氏环定义的要求完全一致.故 $F[x]$是个欧氏环.

例 2 在有理数域 **Q** 上规定,对任意 $a\neq 0$, $d(a)=1$.则 d 是 $\mathbf{Q}_0$ 到 $\mathbf{I}_+$ 的映射;且

(1) 只要 $a,b\neq 0$,恒有 $d(a)=d(b)=1$;

(2) 当 $b\neq 0$ 时,必有 $c\in\mathbf{Q}$,使 $a=bc$,从而有 $a=bc+0$.

所以,对于映射 d, **Q** 是个欧氏环.

例 3 所有形如

$$a+\mathrm{i}b,\quad a,b\in\mathbf{I}$$

的复数是复数环的一个子环,称为**高斯**(Gauss)**环**.可以断言,高斯环是个欧氏环.

用 G 代表高斯环,$1=1+0\mathrm{i}\in G$, G 是个整环.令

$$N(\alpha)=\alpha\bar{\alpha},\quad 对任意 \alpha\in G,$$

其中 $\bar{\alpha}$ 是α 的共轭复数.也就是

$$N(a+\mathrm{i}b)=a^2+b^2,\quad 对每个 a+\mathrm{i}b\in G.$$

首先,$N(a+\mathrm{i}b)=0$,当且仅当 $a+\mathrm{i}b=0$.其次,当 $a+\mathrm{i}b\neq 0$ 时,

$N(a+\mathrm{i}b)\geqslant 1$. 再次，当 $a+\mathrm{i}b\neq 0$, $c+\mathrm{i}d\neq 0$ 时，由

$$
\begin{aligned}
&N((a+\mathrm{i}b)(c+\mathrm{i}d)) \\
&= N(ac-bd+\mathrm{i}(bc+ad)) && \text{(复数乘法)} \\
&= (ac-bd)^2+(bc+ad)^2 && \text{(N 的定义)} \\
&= (ac)^2+(bd)^2+(bc)^2+(ad)^2 && \text{(展开)} \\
&= (a^2+b^2)(c^2+d^2) && \text{(分解)} \\
&= N(a+\mathrm{i}b)N(c+\mathrm{i}d) && \text{(N 的定义)}
\end{aligned}
$$

可得，$N(\alpha\beta)\geqslant N(\alpha)$ 对所有 $\alpha,\beta\in G$ 都成立，即 G 满足定义 2 的条件(1). 最后验证 G 满足定义 2 之条件(2). 任取

$$\alpha=a+b\mathrm{i},\quad \beta=c+d\mathrm{i}\neq 0,$$

我们希望找到 $\sigma,\rho\in G$ 使得

$$\alpha=\beta\sigma+\rho,\quad N(\rho)<N(\beta)\text{ 或 }\rho=0. \qquad (*)$$

分析 如果有(*)成立，那么，由 $\beta\neq 0$，有

$$\rho=\alpha-\beta\sigma=\beta(\alpha/\beta-\sigma).$$

要想使 $N(\rho)<N(\beta)$，只要选择好 σ 使得 $\alpha/\beta-\sigma$ 的模

$$|\alpha/\beta-\sigma|<1. \qquad (**)$$

记 $\alpha/\beta=x+y\mathrm{i}$，其中 x 和 y 都是有理数. 记 $\sigma=e+f\mathrm{i}$. (* *)式就变成要求选好 σ 使，

$$|x+y\mathrm{i}-(e+f\mathrm{i})|=|(x-e)+(y-f)\mathrm{i}|<1.$$

这是能够办到的，只要取 $|x-e|\leqslant\frac{1}{2}$, $|y-f|\leqslant\frac{1}{2}$ 即可.

下面给出(*)式的正式证明.

证明 任取 G 中元

$$\alpha=a+b\mathrm{i},\quad \beta=c+\mathrm{i}d\neq 0.$$

设 $\alpha/\beta=x+y\mathrm{i}$. 其中 x,y 均为有理数. 每个有理数与离它最近的整数的距离当然 $\leqslant\frac{1}{2}$，从而必有整数 e、f 使

$$|x-e|<\frac{1}{2},\quad |y-f|<\frac{1}{2}.$$

令 $\sigma=e+f\mathrm{i}$，则 $\sigma\in G$. 再令 $\rho=\alpha-\beta\sigma$，又有 $\rho\in G$，满足 $\alpha=\beta\sigma+$

ρ. 而且，

$$N(\rho)=N(\alpha-\beta\sigma)=|\beta|^2|\alpha/\beta-\sigma|^2,$$

$$|\alpha/\beta-\sigma|^2=|x-e+(y-f)\mathrm{i}|^2\leqslant\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2<1$$

知道 $N(\rho)<|\beta|^2=N(\beta)$.

命题 3 设 D 对映射 d 是个欧氏环，$a\in D$，$a\neq0$. 那么，a 为单位的充分必要条件是 $d(a)=d(1)$.

证明 如果 a 是 D 的一个单位，即有 c 使 $ac=1$，则

$$\begin{aligned}
d(a)&\leqslant d(ac) && (\text{定义 }2)\\
&=d(1) && (ac=1)\\
&\leqslant d(1\cdot a) && (\text{定义 }2)\\
&=d(a); && (1\text{ 的性质})
\end{aligned}$$

也就是 $d(a)\leqslant d(1)\leqslant d(a)$，$d(a)=d(1)$.

反之，如果 $d(a)=d(1)$，由于有

$$1=aq+r,\quad r=0\text{ 或 }d(r)<d(a),$$

而

$$d(r)<d(a)=d(1)\leqslant d(1\cdot r)=d(r)$$

是不可能的，故必须 $r=0$，$1=aq$，a 为 D 的单位. ▌

定理 2 每个欧氏环都是主理想整环.

证明 设整环 D 对映射 d 是个欧氏环，A 是 D 的一个理想.

如果 $A=\{0\}$，那么，它就是 0 生成的主理想.

如果 $A\neq\{0\}$，它包含非 0 元素，令

$$T=\{d(x)\in\mathbf{I}_+\mid x\in A\}.$$

T 是 A 在映射 d 之下的像. 由于 A 有非 0 元，所以 T 是个非空的非负整数集，它必有最小的元. 设 $a\in A$ 使得 $d(a)$ 是 T 的最小元.

我们断言，$A=(a)$.

$a\in A$，显然有 $(a)\subseteq A$. 任取 $x\in A$，据定义，必有 $q,r\in D$ 使

$$x=aq+r,\quad r=0\text{ 或 }d(r)<d(a).$$

但是，A 是 D 的理想，由 $x,a\in A$ 可知 $aq\in A$ 而且

$$x-aq=r\in A.$$

而 $d(r)<d(a)$ 与 a 的选取相矛盾，故只能 $r=0$，也就是 $x=aq$，$x\in(a)$. 由 x 的任意性推出 $A\subseteq(a)$.

总之，$A=(a)$，A 是个主理想. ▌

这样，我们得到下列环类的关系：

欧氏环类⊆主理想整环类⊆唯一分解整环类⊆整环类.

至于各类之间是否真的不同，也就是给出些具体例子说明，有的主理想整环不是欧氏环，有的唯一分解整环不是主理想整环，等等，也并非难事. 但，这些例子不是初学者十分熟悉的，这里就不予介绍了.

对于欧氏环，讨论其整除性，我们有

命题 4 设 D 对映射 d 为欧氏环，$b\neq0$，$a|b$ 且 a 不是单位也不是和 b 相伴的. 则 $d(a)<d(b)$.

证明 据定义，应有 $q,r\in D$ 使

$$a=bq+r,\quad r=0 \text{ 或 } d(r)<d(b).$$

但，$r=0$ 则意味着 $b|a$，导致 a 是和 b 相伴的，矛盾. 故 $r\neq0$，

$$d(r)<d(b).$$

又 $a|b$，必有 $c\in D$ 使 $b=ac$，从而

$$r=a-bq=a-acq=a(1-cq).$$

用 d 的性质，即得到

$$d(a)\leqslant d(r)<d(b).$$ ▌

在欧氏环中有一种求最大公因子的算法.

例题 2 设 D 对映射 d 是个欧氏环. $a,b\in D$ 且 $b\neq0$. 求 a 和 b 的一个最大公因子.

解 因为 D 是个欧氏环，必有 $q_1,r_1\in D$ 使

$$a=bq_1+r_1,\quad r_1=0 \text{ 或 } d(r_1)<d(b).$$

如果 $r_1=0$，那么 $b|a$，b 即为 a,b 的一个最大公因子.

如果 $r_1\neq0$，则必有 $d(r_1)<d(b)$. 又必有 $q_2,r_2\in D$ 使

$$b=r_1q_2+r_2,\quad r_2=0 \text{ 或 } d(r_2)<d(r_1).$$

当 $r_2=0$ 时,算法即停止;当 $r_2\neq0$ 时,$d(r_2)<d(r_1)$再做

$$r_1=r_2q+r_3,\quad r_3=0 \text{ 或 } d(r_3)<d(r_2).$$

一直做下去.

由于 $d(r_1)>d(r_2)>\cdots$且它们都是非负整数,这种做法不会永远做下去,必然有限步停止;即到某一步,出现整除情况.一般地,可以设

$$\begin{aligned}
&a=bq_1+r_1, && d(r_1)<d(b),\\
&b=r_1q_2+r_2, && d(r_2)<d(r_1),\\
&r_1=r_2q_3+r_3, && d(r_3)<d(r_2),\\
&\cdots,\\
&r_{k-2}=r_{k-1}q_k+r_k, && d(r_k)<d(r_{k-1}),\\
&r_{k-1}=r_kq_{k+1}.
\end{aligned}$$

可以断言 r_k 就是a,b 的一个最大公因子.

首先,$r_k\mid r_{k+1}$,看上列倒数第二个等式,即知 $r_k\mid r_{k-2}$.追溯上去,r_k 可整除每一个 r_i.可是,从第二个等式可以看出 $r_k\mid b$.

再看第一式,由 $r_k\mid b$, $r_k\mid r_1$ 又推知 $r_k\mid a$,也就是说,r_k 是 b 的因子,也是 a 的因子.从而,它是 a,b 的一个公因式.

其次,还需证明 a,b 的任意一个公因子c 可整除r_k.这次,我们从上往下看.

c 是a 和b 的公因子,第一式表明,必有 $c\mid r_1$.于是,在第二式中,由 $c\mid b$, $c\mid r_1$ 可推出 $c\mid r_2$.如此下去,c 必然整除r_k.

所以 r_k 是a,b 的一个最大公因子. ▌

例题 3 求有理数域上多项式

$$a(x)=x^4-x^3-x^2+1,\quad b(x)=x^3-1$$

的最大公因子.

解 做除法,得

$$x^4-x^3-x^2+1=(x^3-1)(x-1)+(-x^2+x),$$

$$x^3-1=(-x^2+x)(-x-1)+(x-1),$$
$$-x^2+x=(x-1)(-x).$$
从而知 $x-1$ 是 $a(x)$和 $b(x)$的一个最大公因子. ▌

例题 4 找出两个整数 m,n 使得 $73m+27n=1$.

解 做长除法,得

$$73=2\times 27+19,$$
$$27=19+8,$$
$$19=2\times 8+3,$$
$$8=2\times 3+2,$$
$$3=2+1,$$

然后,反过来,又有

$$\begin{aligned}1&=3-2\\&=3-(8-2\times 3)\\&=3\times 3-8\\&=3\times(19-2\times 8)-8\\&=3\times 19-7\times 8\\&=3\times 19-7(27-19)\\&=10\times 19-7\times 27\\&=10\times(73-2\times 27)-7\times 27\\&=10\times 73-27\times 27.\end{aligned}$$

从而得到 $10\times 73-27\times 27=1$. ▌

为了加深对高斯整环的认识,我们再讲一个例子.读者可将其与第五章§2 的例 1 加以对照.

例题 5 证明:高斯环 G 同构于环 $\mathbf{I}[x]/(1+x^2)$.

证明 任取 $f(x)\in\mathbf{I}[x]$,用 x^2+1 除之,得

$$f(x)=q(x)(x^2+1)+(\alpha x+\beta).$$

由于 $\alpha x+\beta$ 的次数小于 x^2+1 的次数 2, α 和 β 是由 $f(x)$唯一决定的,令 $\varphi:f(x)\to\alpha\mathrm{i}+\beta$,即得 $\mathbf{I}[x]$到 G 的映射.

仿照第五章§2,容易证明 φ 是个满的环同态映射.

计算 $\mathrm{Ker}(\varphi)$. $f(x)\in\mathrm{Ker}(\varphi)$的充要条件是$(x^2+1)\mid f(x)$，也就是 $f(x)\in(x^2+1)$. 所以

$$\mathrm{Ker}(\varphi)=(x^2+1).$$

由环同态基本定理知 $\mathbf{I}[x]/(x^2+1)\cong G=\mathbf{I}[\mathrm{i}]$. ▌

习 题 二

1. 在 $\mathbf{I}_5[x]$中求

$$x^4+4^*x^3+4^*x^2+1^*,\quad x^3+4^*$$

的一个最大公因子.

2. 设 D 是个主理想整环，$a,b\in D$ 且 a 和 b 互素. 证明：如果 $c\in D$，$a\mid(bc)$，则 $a\mid c$.

3*. 设 R 是个有 1 的交换的主理想环，且 $f:R\rightarrow S$ 是满的环同态映射. 证明：S 必然是主理想环.

4. 求出高斯整环的所有单位.

5. 在高斯整环中把元素 $-1+3\mathrm{i}$ 分解成素元之积.

6. 设 D 对于映射 d 作成一个欧氏环，$a,b\in D$ 且 $a\mid b$. 证明：如果 $d(a)=d(b)$，则 a 和 b 是相伴的.

§3 唯一分解整环上的多项式环

设 F 是个域，那么 F 上的多项式环 $R=F[x]$就是个唯一分解整环.

我们又可以讨论整环 $R=F[x]$上的关于文字 y 的多项式环 $R[y]$，它是否是唯一分解整环呢?

在第五章§4 已经看到，$F[x]$乃是把 F 添上一个与 F"关系疏远"的 x 而成的环. $R[y]$是在 $F[x]$基础上再添一个与 $F[x]$"关系疏远"的 y 而成的环. 这种添两个文字甚至添多个文字的环在数学分析、高等代数及很多进一步的数学学科中都经常出现. 研究 $F[x]$与 $F[x][y]$的关系是很有意义的.

这一节，我们将得到一个很一般的结论，当 R 是唯一分解整

环时，多项式环 $R[x]$ 也一定是个唯一分解整环，进而 $R[x_1,\cdots,x_n]$ 也是个唯一分解整环. 当 F 为域时，当然更是这样.

设 D 是个唯一分解整环，来研究 $D[x]$.

先把一些已知结论总结一下.

1. $D[x]$ 也是个整环，D 的恒等元 1 就是 $D[x]$ 的恒等元；

2. 对任意 $f(x),g(x)\in D[x]$，因 D 无非零的零因子，故

$$\deg[f(x)g(x)]=\deg f(x)+\deg g(x).$$

3. 若 $f(x)\in D[x]$ 是 $D[x]$ 的单位，由 $f(x)g(x)=1$ 知 $f(x)$ 和 $g(x)$ 均为 0 次，即 D 上的常数多项式，

$$f(x)=u,\quad g(x)=v,\quad uv=1.$$

故 $f(x)$ 是 D 的单位. 而 D 之单位当然是 $D[x]$ 的单位. 这说明，$D[x]$ 和 D 有相同的单位.

4. $f(x),g(x)\in D[x]$ 是相伴的，当且仅当，有 D 的单位 c 使

$$f(x)=cg(x).$$

在初等数学中，已经习惯地把“不含次数更低的非常数因式”的多项式称为不可约多项式. 在 $D[x]$ 中，我们把 $D[x]$ 的素元也称为不可约多项式.

但是，当 D 不为域时，并不是 D 中每个非零元均为 $D[x]$ 的单位. 例如，整数环上多项式 $2(x+1)$ 中，2 和 $x+1$ 都是它的非平凡因子. 所以，对唯一分解整环上多项式分解问题的讨论要比在域上讨论来得麻烦，读者必须注意这个细节.

本节恒设 D 是个唯一分解整环. 于是，D 的任意有限多个不全为 0 的元素必有最大公因子.

定义 1 若 1 是多项式

$$f(x)=a_0+a_1x+\cdots+a_nx^n,\quad a_i\in D$$

系数 $a_0,a_1,\cdots,a_n$ 的一个最大公因子，则说 $f(x)$ 是 D 上的一个**本原多项式**.

定理 1(高斯引理) 如果 $g(x),h(x)$ 都是 D 上的本原多项

式，那么它们的乘积

$$f(x)=g(x)h(x)$$

也必为 D 上本原多项式.

证明 设

$$g(x)=a_0+a_1x+\cdots+a_nx^n,$$

$$h(x)=b_0+b_1x+\cdots+b_mx^m$$

都是 D 上本原多项式. 且

$$f(x)=g(x)h(x)=c_0+c_1x+\cdots+c_{m+n}x^{m+n}.$$

如果 $f(x)$ 不是本原多项式，即 $c_0,c_1,\cdots$ 有非单位 d 为其公因子. 将 d 做素因子分解，设 D 的素元 p 是 d 是因子，从而素元 p 是 $c_0,c_1,\cdots,c_{m+n}$ 的一个公因子.

但是，$g(x)$ 和 $h(x)$ 都是本原的，p 不是 $g(x)$ 系数的公因子，p 也不是 $h(x)$ 的系数的公因子. 必有整数 i,j 使 $p\nmid a_i$，$p\nmid b_j$. 设

$$p\mid a_0,\quad p\mid a_1,\quad \cdots,\quad p\mid a_{r-1},\quad p\nmid a_r,$$

$$p\mid b_0,\quad p\mid b_1,\quad \cdots,\quad p\mid b_{s-1},\quad p\nmid b_s.$$

看 $f(x)$ 的系数 c_{r+s}，由于

$$\begin{aligned}c_{r+s}=&a_0b_{r+s}+a_1b_{r+s-1}+\cdots+a_{r-1}b_{s+1}+a_rb_s\\&+a_{r+1}b_{s-1}+\cdots+a_{r+s-1}b_1+a_{r+s}b_0\end{aligned}$$

的右端除 a_rb_s 外其余诸项中或者 a 的脚码小于 r 或者 b 的脚码小于 s，二因子中总有一个要能被 p 整除. 又 $p\mid c_{r+s}$，故 $p\mid(a_rb_s)$.

D 是唯一分解整环，p 为素元，由 §1 之定理 1 知，$p\mid a_r$ 或 $p\mid b_s$，矛盾. ▌

一般来说，如果整环 S 是整环 R 的子环，那么，S 上的多项式 $f(x)$ 也是 R 上的多项式. 而且，可能 $f(x)$ 在 S 上是不可约的，而它作为 R 上的多项式却是可约的.

例如，有理数环 $\mathbf{Q}$ 上多项式

$$f(x)=x^2-2$$

是不可约的，而它作为实数域 $\mathbf{R}$ 上的多项式却有

$$f(x)=(x+\sqrt{2})(x-\sqrt{2}).$$

这样，就为我们的研究提供了一个途径.讨论 S 上一个多项式 $f(x)$ 的性质时，先看它在 R 上的性质，然后再返回到 S 上来做结论.当然，我们不是对任意一个包含 S 的整环 R 都有兴趣，通常是要求 R 比 S"更好".

设 D 是个唯一分解整环，第五章§3提供的方法，有域 Q，$Q\supseteq D$.现在，大家只能知道 $D[x]$ 是个整环，但却知道 $Q[x]$ 是个欧氏环，$Q[x]$ 要比 $D[x]$ 好.

命题 1 设 Q 是 D 的分式域.那么，$Q[x]$ 的非零多项式 $f(x)$ 必可写成如下形式

$$f(x)=\frac{b}{a}f_0(x),$$

其中 $f_0(x)$ 是 $D[x]$ 的本原多项式，$\frac{b}{a}\in Q$.而且，$f_0(x)$ 在不计相伴的意义下是由 $f(x)$ 唯一确定的.

证明 设

$$f(x)=\frac{b_0}{a_0}+\frac{b_1}{a_1}x+\cdots+\frac{b_n}{a_n}x^n,\quad \frac{b_i}{a_i}\in Q,\ \frac{b_n}{a_n}\neq 0.$$

令 $a=a_0a_1\cdots a_n$，则

$$f(x)=\frac{1}{a}[c_0+c_1x+\cdots+c_nx^n],\quad c_i\in D,\ c_n\neq 0.$$

再设 c 是 $c_0,c_1,\cdots,c_n$ 的一个最大公因子，于是

$$f(x)=\frac{c}{a}[d_0+d_1x+\cdots+d_nx^n],\quad d_i\in D,\ d_n\neq 0.$$

此时，1必为 $d_0,d_1,\cdots,d_n$ 的一个最大公因子.若不然，可设 d 为 $d_0,\cdots,d_n$ 的一个最大公因子，d 不是单位，于是 cd 就是 $c_0,c_1,\cdots,c_n$ 的一个公因子，且 cd 不是和 c 相伴的，与 c 之最大性矛盾.

令

$$f_0(x)=d_0+d_1x+\cdots+d_nx^n.\qquad (*)$$

则 $f_0(x)$是 D 上本原多项式，且

$$f(x)=\frac{c}{a}f_0(x),\quad \frac{c}{a}\in Q.$$

进一步，如果还有 D 上本原多项式 $g_0(x)$，

$$f(x)=\frac{h}{f}g_0(x),\quad \frac{h}{f}\in Q.$$

那么研究 D 上多项式，

$$l(x)=fcf_0(x)=hag_0(x). \qquad (**)$$

设 q 是 $l(x)$的所有系数的一个最大公因子. $(**)$表明 fc 是 $l(x)$所有系数的一个公因子，故有

$$(fc)\mid q,\quad q=fct,\ t\in D.$$

又因为 q 是 $fcf_0(x)$诸系数的公因子，注意$(*)$，必有

$$fcd_0=r_0q,\quad \cdots,\quad fcd_n=r_nq.$$

从而得到

$$d_0=r_0t,\quad \cdots,\quad d_n=r_nt.$$

这说明 t 是 $f_0(x)$诸系数的一个公因子. 由于 $f_0(x)$在 D 上是本原的，故 t 必然是个单位. fc 与 q 是相伴的，fc 是多项式 $l(x)$诸系数的一个最大公因子.

同理，ha 也是 $l(x)$诸系数的一个最大公因子. 从而 fc 是与 ha 相伴的，有 D 中单位之使得 $ha=\varepsilon fc$. 将其代入$(**)$，用消去律即得

$$fcf_0(x)=\varepsilon fcg_0(x),\quad f_0(x)=\varepsilon g_0(x);$$

也就是说，如果不考虑相伴的元素的差别时，$f_0(x)$是由 $f(x)$唯一确定的. ▍

命题 2 设 Q 是 D 的分式域. 那么，D 上的本原多项式 $f(x)$ 在 $D[x]$中是可约的，当且仅当，$f(x)$在 $Q[x]$中是可约的.

证明 若 $f(x)$在 $D[x]$中是可约的，即 $f(x)$在 $D[x]$中有非平凡的因子 $h(x)$，即 $h(x)\mid f(x)$且 $h(x)$不是 $D[x]$的单位也不是和 $f(x)$相伴的.

假设 $h(x)$是 $Q[x]$的单位,那么它的次数必为0,它必为 D 的一个常数多项式 c, $c\neq 0$. 于是导出,在 $D[x]$中, $c\mid f(x)$. 而 $f(x)$是 D 上本原多项式,故 c 为 $D[x]$中的单位,与 $h(x)$的假设矛盾.

假设 $h(x)$在 $Q[x]$中是与 $f(x)$相伴的,即有 $c, b\in D$ 使

$$h(x)=\frac{c}{b}f(x),\quad bh(x)=cf(x).$$

若

$$f(x)=a_0+a_1x+\cdots+a_nx^n,$$

则 b 应为 $ca_0, ca_1, \cdots, ca_n$ 的一个公因子. 但由第六章之命题知 $ca_0, \cdots, ca_n$ 的最大公因子是 c,所以 $b\mid c$. 有 d 使 $b=cd$,

$$df(x)=h(x),\quad f(x)\mid h(x)$$

导致 $f(x)$和 $h(x)$在 $D[x]$中是相伴的,矛盾.

这说明 $h(x)$既不是 $Q[x]$的单位也不是 $f(x)$在 $Q[x]$中相伴的, $h(x)$在 $Q[x]$中是 $f(x)$的非平凡因子. $f(x)$在 $Q[x]$中可约.

反过来,若 $f(x)$在 $Q[x]$中是可约的. 设

$$f(x)=g(x)h(x),\quad g(x), h(x)\in Q[x],$$

$g(x)$和 $h(x)$都是 $f(x)$的非平凡因子.

由于域上的非零的常数多项式必为单位,而 $g(x)$和 $h(x)$均非零,所以它们的次数均大于0. 由命题1知,必有 $D[x]$的本原多项式 $g_0(x)$和 $h_0(x)$使

$$g(x)=\frac{b}{a}g_0(x),\quad h(x)=\frac{d}{c}h_0(x),\quad \frac{b}{a}, \frac{d}{c}\in Q.$$

于是 $f(x)=\frac{b}{a}\frac{d}{c}g_0(x)h_0(x)$.

根据定理1可推出 $g_0(x)h_0(x)$也是 D 上的本原多项式. 再据命题1,必有 D 的单位 ε 使

$$f(x)=\varepsilon g_0(x)h_0(x).$$

这里，$\varepsilon g_0(x)$和$h_0(x)$都是D上多项式，均为$f(x)$的因子．$h_0(x)$次数与$h(x)$相同，大于0，$h_0(x)$不是$D[x]$的单位．$\varepsilon g_0(x)$也不是环$D[x]$的单位，从而$h_0(x)$在$D[x]$中不是与$f(x)$相伴的，$h_0(x)$为$f(x)$在$D[x]$中的非平凡因子．即$f(x)$在$Q[x]$中是可约的． ▌

讲到这里，我们可以从代数理论上来解释初等代数中一个因式分解的方法．

大家所熟悉的"十字交叉法"处理问题的步骤是：要在$\mathbf{I}[x]$中分解多项式x^2-6x+6，那么

(1) 设想$x^2-6x+6=(x-a)(x-b)$；

(2) 看a,b可以取怎样的整数使上式成立，必须有

$$ab=6, \quad a+b=6;$$

(3) a和b或为1和6，或为2和3，但却不能满足$a+b=6$，因为$1+6\neq6$，$2+3\neq6$；

(4) 得结论，该多项式在$\mathbf{I}[x]$中是不可约的．

但，在初中的《代数》里，考虑因子分解实际上是在有理数域$\mathbf{Q}$上进行的．上述的4个步骤怎能保证多项式

$$f(x)=x^2-6x+6$$

在$\mathbf{Q}[x]$中不能分解呢？

用命题2，若$f(x)$在$\mathbf{Q}[x]$中可约，则$f(x)$必在$\mathbf{I}[x]$中可约，因为有理数域恰好是整数环的分式域．

在整数环上，上述4个步骤设计是合理的，$f(x)$在$\mathbf{I}[x]$中不可约，保证了它在$\mathbf{Q}[x]$中也是不可约的．

例题1 在有理数域上，多项式$f(x)=x^4+3x+1$是否可约？

解 我们只要看$f(x)$是否在$\mathbf{I}[x]$上可约．

若$f(x)$有一次的非平凡因子

$$f(x)=(ax+b)g(x)$$

比较两端系数，必有$a\mid1$，$b\mid1$，故$ax+b$只可能为

$$x+1, \quad x-1, \quad -x-1, \quad -x+1.$$

两个多项式相差 -1 倍,则是相伴的,故只考虑

$$x+1, \quad x-1.$$

若 $f(x)=(x+1)g(x)$,则 $f(-1)=0$,但 $f(-1)=-1$ 故 $(x+1)\nmid f(x)$. 同理 $(x-1)\nmid f(x)$. 这说明 $f(x)$ 没有一次的非平凡因子.

若 $f(x)$ 有二次的非平凡因子,其首系数必为 ± 1. 相伴的可以不计,$f(x)$ 必有首系数为 1 的二次非平凡因子,故可设有整数 a,b,c,d 使

$$x^4+3x+1=(x^2+ax+b)(x^2+cx+d).$$

于是下列整数方程组应该有解

$$\begin{cases} a+c=0, \\ b+d+ac=0, \\ bc+ad=3, \\ bd=1. \end{cases}$$

但是,这意味着 b,d 同时为 1 或同时为 -1,从而 $b+d=\pm 2$. 同时

$$ac=-a^2=-(b+d),$$

导致 $a^2=\pm 2$,矛盾.

$f(x)$ 在 $\mathbf{Z}[x]$ 上不可约,从而在 $\mathbf{Q}[x]$ 上亦不可约. ∎

命题 3 $D[x]$ 中非常数的本原多项式 $f(x)$ 在 $D[x]$ 中有唯一分解(相伴不计).

证明 首先证明 $f(x)$ 必可写成 $D[x]$ 的不可约多项式之连乘积.

当 $f(x)$ 本身不可约时,目的已经达到.

当 $f(x)$ 可约时,它的非平凡因子不能是常数多项式,故必有

$$g(x), h(x) \in D[x],$$

$$f(x)=g(x)h(x), \quad 1 \leqslant \deg g(x) < \deg f(x).$$

再据 $f(x)$ 的本原性知 $g(x)$ 和 $h(x)$ 均为 $D[x]$ 中本原的.

如果 $g(x)$ 或 $h(x)$ 可约，将其分解，有

$$f(x)=k(x)l(x)j(x),$$

其中 $k(x)$，$l(x)$ 和 $j(x)$ 都是非常数的本原多项式.

由于 $f(x)$ 次数有限，最后可得到

$$f(x)=p_1(x)p_2(x)\cdots p_r(x), \qquad (*)$$

其中 $p_i(x)$ 是 $D[x]$ 上非常数的不可约的本原多项式.

若，又有

$$f(x)=q_1(x)q_2(x)\cdots q_3(x) \qquad (**)$$

其中 $q_j(x)$ 是不可约的. 那么，$q_j(x)$ 必然是本原的. 再由 $f(x)$ 的本原性知 $q_j(x)$ 均不为常数多项式.

根据命题 2，$p_i(x)$，$q_j(x)$ 在 $Q[x]$ 中也是不可约的. 但 Q 是个域，$Q[x]$ 是个唯一分解整环. 在 $Q[x]$ 中看 $(*)$ 和 $(**)$，必有 $r=s$. 调整 $q_j(x)$ 的顺序后，$p_i(x)$ 和 $q_i(x)$ 在 $Q[x]$ 中是相伴的. 设

$$q_i(x)=\frac{b_i}{a_i}p_i(x), \quad \frac{b_i}{a_i}\in Q.$$

在 $D[x]$ 中就有（据命题 1）

$$q_i(x)=\varepsilon_i p_i(x),$$

其中 ε_i 是 D 的单位. 不计相伴的差别，$p_i(x)$ 和 $q_i(x)$ 是 $f(x)$ 的相同的因子. ∎

定理 2 如果 D 是唯一分解整环，则 $D[x]$ 也是唯一分解整环.

证明 任取 $D[x]$ 的一个非 0 非单位的多项式 $f(x)$.

如果 $f(x)$ 是非 0 非单位的常数多项式，即 $f(x)\in D$. 由于 D 是唯一分解整环，$f(x)$ 可以写成 D 的素元的连乘积，也就是 $D[x]$ 的素元之连乘积，且分解唯一.

所以，我们只需考虑 $f(x)$ 不是常数多项式的情形. 设把 $f(x)$ 诸系数之最大公因子提出来，

$$f(x)=dg(x),$$

其中 $g(x)$是 D 上的本原多项式.

如果 d 是D 的一个单位,则 $f(x)$就是 D 上本原多项式,据命题 3,它可唯一地分解.

如果 d 不是D 的单位,d 在D 中唯一分解,设

$$d=p_1p_2\cdots p_m,$$

其中 p_i 都是D 的素元.同样据命题 3,

$$g(x)=p_1(x)\cdots p_r(x),$$

其中 $p_j(x)$都是 $D[x]$的不可约多项式.由于 p_i 也是$D[x]$的素元,

$$f(x)=p_1p_2\cdots p_mp_1(x)p_2(x)\cdots p_r(x).$$

已写成 $D[x]$之素元乘积形式.

设 $f(x)$还有一素元积形式.我们总可以调整顺序,让那些属于 D 的在前,不属于 D 的列后,即不妨设为

$$f(x)=q_1\cdots q_nq_1(x)\cdots q_s(x),$$

其中 $q_i\in D$, $q_j(x)\notin D$.

这里 q_i 是$D[x]$的素元,当然就是 D 的素元.而 $q_j(x)$必然是非常数的本原多项式,否则其系数的最大公因子 d 不是单位,从而是 $q_j(x)$的一个非平凡因子.

于是,先由定理 1 知

$$p_1(x)\cdots p_r(x)\text{和 } q_1(x)\cdots q_s(x)$$

均为本原多项式,再由

$$p_1(x)\cdots p_r(x)=\frac{q_1\cdots q_n}{p_1\cdots p_m}q_1(x)\cdots q_s(x)$$

和命题 1 知有 D 的单位ε 使

$$p_1(x)\cdots p_r(x)=\varepsilon q_1(x)\cdots q_s(x), \qquad (*)'$$

$$\varepsilon p_1p_2\cdots p_m=q_1q_2\cdots q_n. \qquad (**)'$$

把 D 元唯一分解性用到$(**)'$上,得 $m=n$,调整顺序后 p_i 和q_i 是相伴的.

把命题 3 用到 $(*)'$ 上，得 $r=s$，且调整顺序后 $p_i(x)$ 和 $q_i(x)$ 是相伴的.

最终得到 $f(x)$ 的唯一分解性质. ▌

这个定理的证明比较长，而且是步步深入的. 定理包括了前面的命题，通常把前面的命题称为引理，若把它们都写到一个定理里就更长了.

回过头来看这节证明的基本思想，关键是把 $D[x]$ 中的素元分成在 D 中的(常数多项式)和不在 D 中的(非常数多项式)两类，从而引出了本原多项式概念.

处理多项式可约性问题还有很多具体的技巧，初学者难于想到，我们再举几个例子，把它们作为习题留给读者似乎太难了.

例题 2 设 D 是个唯一分解整环，Q 是 D 的分式域，

$$f(x)=a_0+\cdots+a_nx^n\in D[x],$$

如果 $f(x)$ 在 Q 中有一个根 $u/v\in Q$，$u,v\in D$，而且 u 和 v 互素，那么，$u\mid a_0$，$v\mid a_n$.

证明 将 u/v 代入 $f(x)$ 得

$$f(u/v)=a_0+a_1(u/v)+\cdots+a_n(u/v)^n=0.$$

把上式两端同乘 v^n，得

$$a_0v^n+a_1uv^{n-1}+\cdots+a_{n-1}u^{n-1}v+a_nu^n=0.$$

上式左端除第一项 a_0v^n 外，其余诸项均含 u 因子，故亦必有 $u\mid(a_0v^n)$. 由于 u 与 v 互素，u 与 v^n 互素，必有 $u\mid a_0$.

对称地，看等式左端最后一项 a_nu^n，可以证明 $v\mid u^n$. ▌

例题 3 用 φ 代表环 $\mathbf{I}$ 到环 $\mathbf{I}_p$ 的同态映射. 若 $a\in\mathbf{I}$，$a=qp+r$，$0\leqslant r<p$，$\varphi(a)=r^*$，现设 p 是任意取定的一个素数. 对任意一个首系数为 1 的整系数多项式

$$f(x)=a_0+\cdots+x^n\in\mathbf{I}[x],$$

得 $\mathbf{I}_p$ 上多项式

$$\bar{f}(x)=\varphi(a_0)^*+\cdots+1^*x^n.$$

证明:若 $\bar{f}(x)$在 $\mathbf{I}_p[x]$中是不可约的,则 $f(x)$在 $\mathbf{I}[x]$必然是不可约的.

证明 若 $f(x)$在 $\mathbf{I}[x]$上不是不可约的,设 $f(x)=g(x)h(x)$,

$$h(x)=b_0+\cdots+x^m,\quad 0<m<n$$

$$g(x)=c_0+\cdots+x^k,\quad 0<k<n,$$

那么 $\bar{f}(x)=\bar{g}(x)\bar{h}(x)$,其中

$$\bar{h}(x)=\varphi(b_0)^*+\cdots+1^*x^m\in\mathbf{I}_p[x],$$

$$\bar{g}(x)=\varphi(c_0)^*+\cdots+1^*x^k\in\mathbf{I}_p[x],$$

都是 $\bar{f}(x)$的非平凡因子.矛盾. ▎

例如,证明多项式

$$f(x)=x^4+9x^3+6x^2+3x+1$$

在 $\mathbf{I}[x]$中不可约.取 $p=3$,由于 $\varphi(9)=\varphi(6)=\varphi(3)=0^*$,故

$$\bar{f}(x)=1^*x^4+1^*.$$

观查 $\bar{f}(x)$,它不能有一次的因式,因为 $\mathbf{I}_p$ 中任意元 $0^*,1^*,2^*$ 代入 $\bar{f}(x)$都不为 0^*.

如果 $\bar{f}(x)$能分解成二次因子之积.因其首尾系数均为 1^*,其分解只能是

$$x^4+1^*=(x^2+ax+1^*)(x^2+bx+1^*),$$

或者

$$x^4+1^*=(x^2+dx+2^*)(x^2+kx+2^*).$$

计算各项的系数,应有

$$a+b=0^*,\quad ab+2^*=0^*.$$

由于 $ab+2^*=0^*$ 意味着 $ab=1^*$,从而 a,b 必同时为 1^* 或同时为 2^*,故 $a+b\neq 0^*$,导出矛盾.

同理 $x^4+1^*=(x^2+dx+2^*)(x^2+kx+2^*)$亦导出矛盾.

例题 4 设 D 是个整环,那么

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+1\in D[x]$$

在 $D[x]$中不可约的充分必要条件是

$$g(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+1\in D[x]$$

在 $D[x]$ 中不可约.

证明 若有 $h(x),k(x)$ 使 $f(x)=h(x)k(x)$,

$$h(x)=b_0x^m+\cdots+b_m,\quad 1<m<n,$$

$$k(x)=c_0x^l+\cdots+c_l,\quad 1<l<n.$$

那么,$b_mc_l=1$, b_m 和 c_l 均不为 0. 从而

$$p(x)=b_mx^m+\cdots+b_0,$$

$$q(x)=c_lx^l+\cdots+c_0$$

之次数分别为 m 和 l,且 $g(x)=p(x)q(x)$. 这说明,当 $f(x)$ 有非平凡因子时,$g(x)$ 必有非平凡因子. 对称地,当 $g(x)$ 有非平凡因子时,$f(x)$ 也必然有非平凡因子. ∎

习 题 三

1. 证明:多项式 x^4+2x+2 在有理数域 **Q** 上是不可约的.

2. 设 p 是个素数,$f(x),g(x),h(x)\in \mathbf{I}[x]$, $pf(x)=g(x)h(x)$,而且 $g(x)$ 的首系数不能被 p 整除. 证明:$h(x)$ 的每个系数均能被 p 整除.

小 结

由整除问题引出的一系列概念,如整除、相伴、不可约元、素元、因式分解、唯一分解性、最大公因子、互素、主理想整环、欧氏环、高斯整环、本原多项式等等,在代数学的发展史上都出现比较早,起过重要作用.

整除问题起源于对整数性质的研究,整数当然是人类最早知道的"数". 整除问题后来又被推广到数域上的多项式问题的研究,它与解方程问题密切相关.

所以,如果随时注意整数和多项式的性质,对于本章内给出的众多新概念就不会感到太突然和太陌生. 有些命题、定理和习题的证明也就显得相当自然了.

所以，学好本章内容的捷径就是对每个新概念、新命题都要对照地想想它在整数环上应当是怎么回事，在数域上的多项式环中又是怎么回事，分析其异同.温故知新，在分析和借鉴的基础上前进，事情总会好办一些.

本章有一二个定理的证明比较繁复.读者应该先看一下证明的大致步骤，弄清每一步要解决的问题，详细的计算可以先跳过去.然后再分段那些精细的计算，具体弄懂那些系数、数码、方次等等.开始时因符号太多看起来容易眼花缭乱抓不到要领，反复几遍就觉得所要做的事情并不太多.实际上，学习《抽象代数学》最基本的困难不在这些计算性的证明上，只要花工夫，可以相信，这些篇幅长的定理是能被读者接受的.

关于具体的长除法、求最大公因式等，希望读者能把书上的每个例子和例题都看懂，但不要求读者能熟练地去计算和判断是否可约等等.出于这个目的，本章的例题较多，供大家看，而留的习题较少，即不要求大家熟练各种计算方法.

复 习 题

1. 问，在 $\mathbf{I}_5[x]$ 中多项式 x^2+1^*，x^3+x^2+1 是不是素元？

2. 在 $\mathbf{I}_2[x]$ 中求

$$f(x)=x^5+x^4+1^*,\quad g(x)=x^5+x+1^*$$

的一个最大公因子 d，并找出 $k,l\in\mathbf{I}_2[x]$ 使 $kf(x)+lg(x)=d$.

3. 设整环 D 对于映射 d 是个欧氏环，而 c 是个正整数，对任意 $x\in D$，令 $d'(x)=d(x)+c$.则 d' 也是 D_0 到 $\mathbf{I}_+$ 的映射，且 D 对于 d' 也是个欧氏环.

4. 设 D 为整环，$a,b,q,r\in D$，且 $a=bq+r$.证明：若有 $d\in D$ 则 $d\mid a$ 且 $d\mid b$ 的充分必要条件是 $d\mid b$ 且 $d\mid r$.

第七章　域的扩张

这一章讨论一个域和它的子域以及它的扩域之间的关系.

学习群论时，重点讨论正规子群而不是一般子群，学习环论时，重点讨论环的理想而不是一般子环. 那么，是不是因为域不含非平凡理想，而只好研究它的子域呢?

研究域与其扩域之间的关系不是仿照群论或环论进行纯理论推演，历史上，它来自于处理“解方程问题”.

一百五十多年前，伽罗华(Galois)首先利用域的扩张理论探讨了“关于用根式解方程的可解性条件”，为现代抽象代数学的发展奠定了基础. 他的天才思想和巧妙方法透彻地解决了使很多大数学家伤透脑筋的“根号求解”、“用规尺将任意角三等分”等大难题.

本章内容是域论的基础知识，有了这些知识和技能训练后，有兴趣的读者再去钻研 Galois 理论及其应用，就容易多了.

在这一章里，需要反复使用多项式、剩余环等工具，而这些东西是分散出现在第四章至第六章的. 读者学习本章之前应该把上述三章好好总结一下.

§1　单纯扩张域

我们知道，如果 F,E 都是域，而 F 是 E 的子域，则说 E 是 F 的扩张域，简称扩域.

复数域是实数域的扩张域，复数域和实数域都是有理数域的扩张域.

任何域都是其素域的扩张域.

定义 1 设 E 是 F 的一个扩张域, S 是 E 的一个子集, 由 $F\cup S$ 在 E 中生成的子域, 记为 $F(S)$, 称为是 F 上添加 S 得到的 E 的子域. 当 $S=\{a_1,a_2,\cdots,a_n\}$ 时, 记 $F(S)=F(a_1,a_2,\cdots,a_n)$. 当 $E=F(a)$ 时, 说 E 是 F 的一个**单纯扩张域**, 或说 E 是 F 的一个**单纯扩张**.

例如, 复数域 $\mathbf{C}$ 是实数域 $\mathbf{R}$ 添加一个复数 $\mathrm{i}=\sqrt{-1}$ 而成的, 故 $\mathbf{C}=\mathbf{R}(\mathrm{i})$.

现在看 $\mathbf{R}$ 的单纯扩张 $\mathbf{R}(2+\sqrt{-3})$. 由于

$$2+\sqrt{-3}=2+\sqrt{3}\mathrm{i}\in\mathbf{R}(\mathrm{i}),$$

所以 $\mathbf{R}(2+\sqrt{-3})\subseteq\mathbf{R}(\mathrm{i})$. 另一方面,

$$\mathrm{i}=[(2+\sqrt{3}\mathrm{i})-2]\frac{1}{\sqrt{3}}\in\mathbf{R}(2+\sqrt{-3})$$

知, $\mathbf{R}(\mathrm{i})\subseteq\mathbf{R}(2+\sqrt{-3})$. 故 $\mathbf{R}(\mathrm{i})=\mathbf{R}(2+\sqrt{-3})$.

这说明, 同一个域上不同的添加可能得到相同的扩张域.

为了弄清域 F 上单纯扩张 $E=F(a)$ 的结构, 让我们回忆一下第五章 §4 给出的一个环的同态映射

$$\varphi: f(x)\to f(a),\quad a\in E$$

即

$$\varphi: a_0+a_1x+\cdots+a_nx^n\to a_0+a_1a+\cdots+a_na^n,$$

这是环 $F[x]$ 到 E 的一个环同态映像. 把它的像 $\mathrm{Img}(\varphi)$ 记为 $F[a]$, 即

$$F[a]=\{f(a)\mid f(x)\in F[x]\};$$

或直接写出来, 就是

$$F[a]=\{a_0+a_1a+\cdots+a_na^n\mid \text{任意 } a_0,\cdots,a_n\in F\}.$$

命题 1 设 F 是个域, E 是 F 的单纯扩张, $E=F(a)$. 那么, 或者 E 同构于 $F[x]$ 的分式域 $F\{x\}$, 或者有 F 上的不可约多项式 $p(x)$, 使

$$F(a)\cong F[x]/(p(x)).$$

证明 看 E 的子集，

$$S=\{f(a)g(a)^{-1}\in E\mid f(x),g(x)\in F[x],\ g(a)\neq 0\}.$$

任取 $s_1,s_2\in S$，设

$$s_1=f_1(a)g_1(a)^{-1},\quad f_1(x),g_1(x)\in F[x],\ g_1(a)\neq 0,$$

$$s_2=f_2(a)g_2(a)^{-1},\quad f_2(x),g_2(x)\in F[x],\ g_2(a)\neq 0.$$

在 E 中运算，有

$$s_1-s_2=[f_1(a)g_2(a)-f_2(a)g_1(a)][g_1(a)g_2(a)]^{-1},$$

其中 $g_1(a)g_2(a)\neq 0$，故 $s_1-s_2\in S$. 同样

$$s_1s_2=[f_1(a)f_2(a)][g_1(a)g_2(a)]^{-1},$$

其中 $g_1(a)g_2(a)\neq 0$，故 $s_1s_2\in S$.

进一步，若有 $s\in S$，

$$s=f(a)g(a)^{-1}\neq 0,$$

那么，在域 E 中，$f(a)\neq 0$. 从而

$$s^{-1}=g(a)f(a)^{-1}\in S.$$

所以，S 是个域.

如果 S^* 是 E 的一个子域，$F\cup\{a\}\subseteq S^*$，由于它是个环，所以，对任意 $a_0,\cdots,a_n\in F$，必有

$$a_0+a_1a+\cdots+a_na^n\in S^*;$$

也就是对任意 $f(x)\in F[x]$，必有 $f(a)\in S^*$. 若又有 $g(x)\in F[x]$，那么 $g(a)\in S^*$. 而 S^* 是个域，所以，只要 $g(a)\neq 0$，则

$$f(a)g(a)^{-1}\in S^*.$$

这说明，$S\subseteq S^*$. 由于 S 是 E 的子域且包含在每个含 $F\cup\{a\}$ 的子域中，故 S 就是 E 中 $F\cup\{a\}$ 生成的子域 $F(a)$.

进一步观察 S. $F[a]$ 是 S 的子环，而且 S 是 E 中包含 $F[a]$ 的最小子域（任何子域含 $F[a]$ 则必含 S），据第五章§3之例题1知 S 是环 $F[a]$ 的分式域.

再来研究环 $F[a]$. 由于 $\varphi: f(x)\mapsto f(a)$ 是环 $F[x]$ 到 $F[a]$

的满的环同态，据环同态基本定理，应有

$$F[a]\cong F[x]/\mathrm{Ker}\varphi.$$

这样一来，$F[a]$的结构就决定于 $F[x]$的理想 $\mathrm{Ker}(\varphi)$了. 由于 $F[x]$是主理想环，必有 F 上多项式 $p(x)$使 $\mathrm{Ker}\varphi=(p(x))$. 因为 $F[a]\subseteq E$，E 是个域，故 $F[a]$不含非零的零因子，从而环 $F[x]/\mathrm{Ker}(\varphi)$亦不含非零的零因子，据第六章§2之命题2，$p(x)$或为零多项式，或为 $F[x]$的单位(非零的常数多项式)或为不可约多项式.

若 $p(x)$为 $F[x]$的单位，那么$(p(x))=F[x]$，φ 为零同态，矛盾. 故我们只需分别讨论以下两种情形.

若 $p(x)=0$，$\mathrm{Ker}(\varphi)=\{0\}$，则 $F[x]\cong F[a]$，由第五章§3例题1知 $F[x]$的分式域 $F\{x\}$同构于 $F[a]$的分式域 $S=F[a]$.

若 $p(x)$是 F 上不可约多项式. 那么，环 $F[x]/(p(x))$本身已经是个域(此时$(p(x))$是 $F[x]$之一极大理想)，而 $F[a]$同构于$F[x]/(p(x))$，所以 $F[a]$本身是个域. 由于 $F(a)$是 E 的含a又含F 的所有子域之交集，故 $F[a]\subseteq F(a)\subseteq F[a]$，$F(a)=F[a]$. 最后知道 $F(a)$是个域，且

$$F(a)\cong F[x]/(p(x)),$$

其中 $p(x)$是 F 上不可约多项式. ▌

这个命题告诉我们，给定了域 F，它上面的单纯扩张只有两种. 那么，这两种之间的差别是怎样造成的呢? 关键是映射

$$\varphi: f(x)\to f(a)$$

的核. $\mathrm{Ker}\varphi=\{0\}$意味着对任意非零多项式 $f(x)$都有 $f(a)\neq 0$. $\mathrm{Ker}\varphi=\{p(x)\}$意味着，有 F 上的不可约多项式，使

(1) $p(a)=0$;

(2) 任意 $g(x)\in F[x]$，若 $g(a)=0$，则 $g(x)\in(p(x))$.

定义 2 设域 E 是域F 的扩张域，$a\in E$. 如果有 F 上非零多项式$f(x)$使 $f(a)=0$，则说 a 是F 上的一个**代数元**；如果对 F 上的任意一个非零多项式 $f(x)$都有 $f(a)\neq 0$，则说 a 是F 上的一

个超越元.

命题 2 设 E 是域 F 的扩张域. 如果 $a\in E$ 是 F 上的代数元, 则必有 F 上不可约多项式 $p(x)$ 使得

(1) $p(a)=0$;

(2) 任意 $f(x)\in F[x]$, 只要 $f(a)=0$, 则 $f(x)\in(p(x))$, 即 $p(x)\mid f(x)$.

证明 若 a 是 F 上代数元, 设 $g(x)\in F[x]$, $g(x)\neq 0$ 且 $g(a)=0$. 这说明 a 不是 F 上的超越元. 由命题 1 的证明可看出

$$\varphi: f(x)\to f(a),\quad f(x)\in F[x],$$

$\mathrm{Ker}(\varphi)\neq\{0\}$. 那么, 必有不可约多项式 $p(x)$ 使

$$\mathrm{Ker}(\varphi)=(p(x)).$$

它等价于 $p(x)$ 满足(1)和(2). ▌

当 a 是 F 上代数元, 满足命题 2 条件(1)和(2)的不可约多项式 $p(x)$ 就称为是 a 的一个**极小多项式**, 或**最小多项式**. $F(a)$ 称为 F 的单纯代数扩张, 它同构于域 $F[x]/(p(x))$.

例如, 实数域 $\mathbf{R}$ 中, $\sqrt{5}$ 是有理数域上的一个代数元, 因为它满足 $\mathbf{Q}$ 上多项式

$$f(x)=x^2-5.$$

所以, $\mathbf{Q}(\sqrt{5})$ 是 $\mathbf{Q}$ 上的一个单纯代数扩张.

下面来说明 x^2-5 是 $\mathbf{Q}$ 上不可约多项式. 在第六章 §3, 我们已经知道, x^2-5 在 $\mathbf{Q}$ 上可约当而且仅当, 它在整数环 $\mathbf{I}$ 上可约. 作为 $\mathbf{I}$ 上多项式, x^2-5 如果是可约的, 不计单位(即 ± 1)的差别, 它只能写成

$$x^2-5=(x+a)(x+b),\quad a,b\in\mathbf{I}.$$

从而要求 $a+b=0$, $ab=-5$, 这在整数环 $\mathbf{I}$ 上是办不到的. 所以, x^2-5 是 $\mathbf{Q}$ 上不可约多项式.

事实上, 知道 $\sqrt{5}$ 满足不可约多项式 x^2-5 即可认定 x^2-5 是 $\sqrt{5}$ 在 $\mathbf{Q}$ 上的一个极小多项式. x^2-5 满足命题 2 条件(2)是自然

的. 因为, 当知道$\sqrt{5}$满足 x^2-5 后, 即知$\sqrt{5}$为 $\mathbf{Q}$ 上代数元. 从而必有极小多项式 $p(x)$满足(1)和(2). 从而

$$x^2-5\in(p(x)),\quad p(x)\mid(x^2-5).$$

但 $p(x)$与 x^2-5 均不可约, 它们必然是相伴的,

$$(x^2-5)=(\varphi(x)).$$

推论 1 如果 a 是域F 上的代数元, 那么, a 在F 上的各极小多项式都是相伴的. ▌

事实上, a 的每个极小多项式都是不可约的, 而且要相互整除.

推论 2 设 $F(a)$和 $F(b)$都是域 F 的单纯代数扩张. 如果 a 的极小多项式和b 的极小多项式是相伴的, 那么 $F(a)\cong F(b)$.

证明 设 $p(x)\in F[x]$是 a 的一个极小多项式, 由于 b 的极小多项式是和 $p(x)$相伴的, 所以 $p(x)$也是 b 的一个极小多项式.

看命题 1 的证明, 计算映射 $\varphi: g(x)\to g(a)$的核. 由于 $p(a)=0$, 且对任意 $f(x)\in F[x]$, 只要 $f(a)=0$, 则必有 $f(x)\in(p(x))$, 故 $\mathrm{Ker}\varphi=(p(x))$, 且

$$F[a]=F(a)\cong F[x]/(p(x)).$$

同理, 又有

$$F[b]=F(b)\cong F[x]/(p(x)).$$

所以, $F(a)\cong F(b)$. ▌

现在, 我们反过来问, 给定一个域 F 后, 对 F 上的一个确定的不可约多项式 $p(x)$, 是否一定有 F 的单纯代数扩张$F(a)$使得

$$F(a)\cong F[x]/(p(x))$$

成立呢? 回答是肯定的.

定理 1 设 F 是个域, $p(x)$是 F 上不可约多项式. 那么, 必有 F 上的一个单纯代数扩张域 $F(\lambda)$同构于 $F[x]/(p(x))$, 且 $p(x)$是 λ 在F 上的一个极小多项式.

证明 仿照抽象定义多项式的方法, 看形如下的表达式($n=$

$\deg p(x)$),

$$a_0 \# a_1\lambda \# \cdots \# a_{n-1}\lambda^{n-1}, \qquad (*)$$

其中 $a_0, a_1, \cdots, a_{n-1} \in F$. 规定，当 $a_i = 0$ 时，表达式中 $a_i\lambda^i$ 可以不写；表达式（$*$）和表达式

$$b_0 \# b_1\lambda \# \cdots \# b_{n-1}\lambda^{n-1}. \qquad (**)$$

相等，当且仅当 $b_0 = a_0, \cdots, b_{n-1} = a_{n-1}$.

所有这种表达式的集合记为 E.

据第五章§4命题6，域 $F[x]/(p(x))$ 的每个元素可唯一地表示成

$$c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + (p(x)).$$

建立映射

$$\varphi: c_0 + \cdots + c_{n-1}x^{n-1} + (p(x)) \to c_0 \# \cdots \# c_{n-1}\lambda^{n-1},$$

这是域 $F[x]/(p(x))$ 到集合 E 的一个映射，而且是个双射，它有逆映像 φ^{-1}.

现在来"硬性"规定 E 上的运算使其也成为一个域. 任取 $a, b \in E$. 由于 φ 是双射，必有唯一确定的 $a', b' \in F[x]/(p(x))$ 使得

$$\varphi(a') = a, \varphi(b') = b.$$

我们定义 E 上加法，

$$a \# b = \varphi(a' + b') = \varphi(\varphi^{-1}(a) + \varphi^{-1}(b)),$$

和乘法

$$a \odot b = \varphi(a' \cdot b') = \varphi(\varphi^{-1}(a)\varphi^{-1}(b)).$$

很容易验证$(E, \#, \cdot)$是个域. 而且 $F[x]/(p(x))$ 同构于 E. 细节的验证是机械的、容易的. 可以仿照第三章§2之例题7进行.

注意，形式表达式

$$a_0 \# a_1\lambda \# \cdots \# a_{n-1}\lambda^{n-1}$$

中等于0的 a_i 可以不写. 所以，对任意 $a_0 \in F$,

$$a_0 = a_0 \# 0\lambda \# \cdots \# 0\lambda^{n-1} \in E.$$

即 F 是 E 的子集. 而且，对任意 $a_0, b_0 \in F$，有

$$a_0 \# b_0$$
$$= \varphi[\varphi^{-1}(a_0) + \varphi^{-1}(b_0)] \quad (\# 的定义)$$
$$= \varphi[a_0 + b_0] \quad (\varphi 的定义)$$
$$= a_0 + b_0. \quad (\varphi 的定义)$$

同理可证，$a_0 \odot b_0 = a_0 b_0$. 这说明 F 的运算恰好与它的元素在 E 中运算一样. 所以，F 是 E 的子域.

因为 E 的每个元素

$$a_0 \# a_1\lambda \# \cdots \# a_{n-1}\lambda^{n-1}$$

恰好等于 $a_0, a_1\lambda, \cdots, a_{n-1}\lambda^{n-1}$ 的和，而且 E 已经是个域，故 $E \subseteq F(\lambda)$，进而 $E = F(\lambda)$.

把 E 中元素

$$\lambda = 0 \# 1\lambda \# 0\lambda^2 \# \cdots \# 0\lambda^{n-1}$$

代到 F 上多项式 $p(x)$ 中，记 $I = (p(x))$. 由于 $\varphi: x + I \to \lambda$ 可知

$$p(\lambda) = p(\varphi(x+I)).$$

而 φ 是环同态映射，故 $p(\varphi(x+I)) = \varphi(p(x+I))$. 而映射 $\sigma: x \to x + I$ 是自然同态，$p(x+I) = p(x) + I = I$. 所以，

$$p(\lambda) = \varphi(p(x+I)) = \varphi(I) = 0,$$

即 λ 满足 $p(x)$. 因为 $p(x)$ 在 F 上是不可约的，$p(x)$ 必为 λ 的一个极小多项式. ▌

对于域 F 上单纯扩张的另一种情形. $F[x]$ 的分式域 $F\{x\}$ 为域，且

$$F \subseteq F[x] \subseteq F\{x\},$$

$F\{x\}$ 就是 F 的一个单纯扩张域，x 为 F 上的超越元. $F\{x\}$ 是 F 添加 x 所得的扩张域，故

$$F(x) = F\{x\}.$$

这两个符号就是一样的了(见第五章 §4).

例题 1 证明：域 $\mathbf{I}_2$ 上多项式 $1 + x + x^2$ 是不可约的，给出 $\mathbf{I}_2$ 的一个单纯代数扩张 E，

$$E\cong \mathbf{I}_2/(1+x+x^2).$$

证明 因为 1^*+x+x^2 是 $\mathbf{I}_2$ 上的二次多项式，若可约，则必表成 2 个一次多项式之积，$\mathbf{I}_2$ 上的一次多项式首系数均为 1^*，故

$$p(x)=x^2+x+1^*=(x+a)(x+b).$$

于是应有 $a\in\mathbf{I}_2$ 使 $p(a)=p(-a)=0^*$．但，这是不可能的，因为

$$p(0^*)=1^*,\quad p(1^*)=1^*.$$

由于 x^2+x+1^* 次数为 2，令

$$E=\{0^*,1^*,\lambda,1^*\#\lambda\}.$$

建立映射 $\varphi:F[x]/(p(x))\to E$，

$$(p(x))\to 0^*,\quad 1^*+(p(x))\to 1^*,$$

$$x+(p(x))\to\lambda,\quad (1^*+x)+(p(x))\to 1^*\#\lambda.$$

然后，规定，右面 E 中元素"按照"左面元素在 $F[x]/(p(x))$ 运算实行运算．

如，计算 $1^*\#(1^*\#\lambda)$，先看

$$1^*+(p(x))+(1^*+x)+(p(x))=x+(p(x)),$$

故知 $1^*\#(1^*\#\lambda)=\lambda$．

又如，计算$(1^*\#\lambda)(1^*\#\lambda)$，先看

$$\begin{aligned}
&[(1^*+x)+(p(x))]\cdot[(1^*+x)+(p(x))]\\
&=(1^*+x)(1^*+x)+(p(x))\\
&=(1^*+x^2)+(p(x))\\
&=x+(1^*+x+x^2)+(p(x))\\
&=x+(p(x)).
\end{aligned}$$

从而$(1^*\#\lambda)(1^*\#\lambda)=\lambda$．

具体列出 E 的加法表和乘法表

#	0^*	1^*	λ	$1^*\#\lambda$
0^*	0^*	1^*	λ	$1^*\#\lambda$
1^*	1^*	0^*	$1^*\#\lambda$	λ
λ	λ	$1^*\#\lambda$	0	1^*
$1^*\#\lambda$	$1^*\#\lambda$	λ	1^*	0

$\cdot$	0^*	1^*	λ	$1^* \# \lambda$
0^*	0^*	0^*	0^*	0^*
1^*	0^*	1^*	λ	$1^* \# \lambda$
λ	0^*	λ	$1^* \# \lambda$	1^*
$1^* \# \lambda$	0^*	$1^* \# \lambda$	1^*	λ

从定理 1 的证明和例题 1 的具体计算都可以看出来，E 的元素 λ 符号的选择是无关紧要的，关键是它的运算.

比如，对于 $\mathbf{Q}$ 上的不可约多项式 x^2-2 和 x^2-5，都可令

$$E=\{a\lambda+b \mid a,b\in\mathbf{Q}\},$$

它按不同的办法定义运算后

$$(E,\#,\circ)\cong F[x]/I,\quad I=(x^2-2),$$

$$(E,+,\cdot)\cong F[x]/J,\quad J=(x^2-5).$$

取两个元素 $1-2\lambda,2+\lambda\in E$，计算

$$\begin{aligned}&[(1-2x)+I]+[(2+x)+I]\\&=(1-2x)(2+x)+I\\&=(2-3x-2x^2)+I\\&=(-2-3x)+I,\end{aligned}$$

所以，$(1-2\lambda)\circ(2+\lambda)=-2-3\lambda$. 而

$$\begin{aligned}&[(1-2x)+J]\cdot[(2+x)+J]\\&=(2-3x-2x^2)+J\\&=(-8-3x)+J,\end{aligned}$$

从而 $(1-2\lambda)\cdot(2+\lambda)=-8-3\lambda$.

如同在多项式理论中文字 x 的选择无关紧要一样，我们也可以不让 λ 出现，用抽象形式做出域上某个不可约多项式的单纯代数扩张域.

例 1 把有理数域 $\mathbf{Q}$ 中的每个数 a 换个写法，记为 $(a,0)$，其中 0 就是数零. 于是 $\mathbf{Q}$ 可以看成是集合 $\mathbf{Q}\times\mathbf{Q}$ 的子集.

现在 $\mathbf{Q}\times\mathbf{Q}$ 上定义运算，对任意 $(a,b),(c,d)\in\mathbf{Q}\times\mathbf{Q}$，规定

$$(a,b)+(c,d)=(a+c,b+d),$$
$$(a,b)\cdot(c,d)=(ac+2bd,ad+bc).$$
下面来说明$(\mathbf{Q}\times\mathbf{Q},+,\cdot)$是个域.

首先,建立$\mathbf{Q}[x]$到$\mathbf{Q}\times\mathbf{Q}$的映射,任取$f(x)\in\mathbf{Q}[x]$,用$x^2-2$除之,设为
$$f(x)=q(x)(x^2-2)+bx+a,$$
其中$q(x)\in\mathbf{Q}[x]$,$a,b\in\mathbf{Q}$ 由于$bx+a$是带余除法的余式,是由$f(x)$唯一确定的,从而元素(a,b)亦由$f(x)$唯一确定.令
$$\varphi:f(x)\to(a,b),$$
则φ是$\mathbf{Q}[x]$到$\mathbf{Q}\times\mathbf{Q}$的一个映射.

其次,可以断言φ为环$\mathbf{Q}[x]$到$(\mathbf{Q}\times\mathbf{Q},+,\cdot)$的同态映射.任取$f(x),g(x)\in\mathbf{Q}[x]$,设
$$f(x)=q(x)(x^2-2)+bx+a,$$
$$g(x)=p(x)(x^2-2)+dx+c.$$
那么,
$$f(x)+g(x)=[p(x)+q(x)](x^2-2)+(b+d)x+(a+c),$$
$$\begin{aligned}f(x)g(x)&=t(x)(x^2-2)+(bx+a)(dx+c)\\&=t(x)(x^2-2)+bdx^2+(ad+bc)x+ac\\&=[t(x)-bd](x^2-2)+(ad+bc)x+(ac+2bd).\end{aligned}$$
从而有
$$\begin{aligned}\varphi(f(x)+g(x))&=(a+c,b+d)=(a,b)+(c,d)\\&=\varphi(f(x))+\varphi(g(x)).\end{aligned}$$
同时
$$\begin{aligned}&\varphi(f(x)g(x))\\&=(ac+2bd,ad+bc)\qquad(\text{据}\ \varphi\ \text{的定义和}(*)\text{算式})\\&=(a,b)\cdot(c,d)\qquad(\mathbf{Q}\times\mathbf{Q}\ \text{上乘法的定义})\\&=\varphi[f(x)]\varphi[g(x)].\qquad(\varphi\ \text{的定义})\end{aligned}$$
最后,很容易看出φ是个满射,因为
$$\varphi[bx+a]=(a,b).$$

据第四章§4 例题 6,即知$(\mathbf{Q}\times\mathbf{Q},+,\cdot)$是个结合环.$(0,0)$是$\mathbf{Q}\times\mathbf{Q}$的零元,$(1,0)$是恒等元.

要证明$(\mathbf{Q}\times\mathbf{Q},+,\cdot)$是个域,可研究$\varphi$的核.由于$f(x)\in\mathrm{Ker}(\varphi)$必要而且只要$[x^2-1]\mid f(x)$,故

$$\mathrm{Ker}(\varphi)=(x^2-1).$$

由环同态基本定理知

$$(\mathbf{Q}\times\mathbf{Q},+,\cdot)\cong\mathbf{Q}[x]/(x^2-1).$$

又因为x^2-1是$\mathbf{Q}$上的不可约多项式,所以,环$(\mathbf{Q}\times\mathbf{Q},+,\cdot)$是个域.

开始时我们就说过,$\mathbf{Q}$可以视为$\mathbf{Q}\times\mathbf{Q}$的子集,元素$a$与$(a,0)$是同一元素之不同记法而已.故,$(\mathbf{Q}\times\mathbf{Q},+,\cdot)$是$\mathbf{Q}$的一个单纯代数扩张.

再来看$\mathbf{Q}\times\mathbf{Q}$的元素$(0,1)$.将其代入到$\mathbf{Q}$上多项式$x^2-2$中去,得

$$\begin{aligned}
&(0,1)^2-2(1,0)\\
&\quad=(0,1)\cdot(0,1)-(2,0) && (\mathbf{Q}\times\mathbf{Q}\text{中运算})\\
&\quad=(2,0)-(2,0) && (\text{乘法定义})\\
&\quad=(0,0). && (\text{加法之定义})
\end{aligned}$$

也就是说$(0,1)$满足$\mathbf{Q}$上不可约多项式x^2-2.

由于$(0,1)^2=(2,0)$,按习惯,人们把$(0,1)$记成$\sqrt{2}$.于是

$$\mathbf{Q}\times\mathbf{Q}=\mathbf{Q}(\sqrt{2}).$$ ▌

这个例子中完全不必选择不定元x的符号,也不必选择添加元λ的记法.因为,在多项式理论的讨论中,我们已经看到,不定元x只起标记各系数位置的作用.如同在第五章§4 例 4 的做法一样,用序列记多项式,那么,在研究域的扩张时,也可以回避x和λ等记号.

这可以再给一个差不多是重复的例子.

例 2 把实数域$\mathbf{R}$中元素a记为$(a,0)$,其中 0 是数零.

对$\mathbf{R}\times\mathbf{R}$中任意元$(a,b)$和$(c,d)$规定

$$(a,b)+(c,d)=(a+c,b+d),$$
$$(a,b)\cdot(c,d)=(ac-bd,ad+bc).$$
则$(\mathbf{R}\times\mathbf{R},+,\cdot)$有了两个二元运算.

建立$\mathbf{R}[x]$到$\mathbf{R}\times\mathbf{R}$的映射$\varphi$,若$f(x)\in\mathbf{R}[x]$,
$$f(x)=q(x)(x^2+1)+bx+a,$$
其中$q(x)\in\mathbf{R}[x]$, $a,b\in\mathbf{R}$.规定
$$\varphi:f(x)\to(a,b)$$
则φ是$\mathbf{R}[x]$到$\mathbf{R}\times\mathbf{R}$的一个映射,而且是满的.

如果$f(x),g(x)\in\mathbf{R}[x]$,
$$f(x)=q(x)(x^2+1)+bx+a,$$
$$g(x)=p(x)(x^2+1)+dx+c,$$
那么,可以算出(读者应仔细计算之)
$$\varphi[f(x)+g(x)]=(a+c,b+d)=\varphi[f(x)]+\varphi[g(x)],$$
$$\varphi[f(x)g(x)]=(ac-bd,ad+bc)=\varphi[f(x)]\varphi[g(x)].$$
于是知,$(\mathbf{R}\times\mathbf{R},+,\cdot)$是个环.而$\mathrm{Ker}(\varphi)=(x^2+1)$,再据环同态基本定理,立得
$$\mathbf{R}\times\mathbf{R}\cong\mathbf{R}[x]/(x^2+1).$$
由于x^2+1在实数域上是不可约多项式,所以$(\mathbf{R}\times\mathbf{R},+,\cdot)$是个域.

进一步,由于$\mathbf{R}$中元已记为$(a,0)$形式,$\mathbf{R}$是$(\mathbf{R}\times\mathbf{R},+,\cdot)$的子域.$\mathbf{R}\times\mathbf{R}$是实数域$\mathbf{R}$的一个单纯代数扩张.

$(0,0)$是$\mathbf{R}\times\mathbf{R}$的零元,$(1,0)$是$\mathbf{R}\times\mathbf{R}$的恒等元.且
$$(0,1)^2+(1,0)=(-1,0)+(1,0)=(0,0),$$
也就是说,$\mathbf{R}\times\mathbf{R}$的元素$(0,1)$满足$\mathbf{R}$上的不可约多项式$x^2+1$.从而$\mathbf{R}\times\mathbf{R}=\mathbf{R}((0,1))$.

习惯上,把平方等于数-1的复数记为i或$\sqrt{-1}$,
$$\mathbf{R}\times\mathbf{R}=\mathbf{R}(\mathrm{i})=\mathbf{R}(\sqrt{-1}).$$
我们得到的扩张$\mathbf{R}\times\mathbf{R}$就是复数域.

由于人们在初等数学中把多项式写成带有不定元形式，本书正文亦遵从此惯例.

定理 2 设 E 是域 F 的一个扩张域. $S, T\subseteq E$，那么，

$$F(S)(T)=F(S\cup T).$$

分析 $F(S)$ 是域 F 添加 E 的子集 S 后得到 E 的子域. 把它再添加上 T，得 $F(S)(T)$. 此子域包含 F, S, T，从而它包含了 E 中由 $F\cup S\cup T$ 生成的子域 $F(S\cup T)$.

关键是要证明 $F(S)(T)\subseteq F(S\cup T)$.

证明 因为 $S\subseteq S\cup T$，故

$$F(S)\subseteq F(S\cup T).$$

这说明 $F(S)$ 是 $F(S\cup T)$ 的子域，且 $T\subseteq F(S\cup T)$，从而

$$F(S)\cup T\subseteq F(S\cup T).$$

而 $F(S)(T)$ 是 E 中包含 $F(S)\cup T$ 的所有子域之交集，从而

$$F(S)(T)\subseteq F(S\cup T).$$

这表明

$$F(S\cup T)=F(S)(T). \quad \blacksquare$$

推论 设 E 是域 F 的一个扩张域，$a_1,\cdots,a_n\in E$. 那么

$$F(a_1,a_2,\cdots,a_n)=F(a_1)(a_2)\cdots(a_n). \quad \blacksquare$$

例题 2 设 F 是个域. 给出 F 中由元素 $a_1,a_2,\cdots,a_n$ 生成的子域 S 的元素表达形式.

解 设 P 是 F 的素域，那么，P 是 S 的子域，S 可以看成是 P 添加 $a_1,a_2,\cdots,a_n$ 而得，即

$$S=P(a_1,a_2,\cdots,a_n).$$

由第五章 §4 知 $P[a_1,a_2,\cdots,a_n]$ 是 F 的子环，

$$P[a_1,\cdots,a_n]=\{f(a_1,\cdots,a_n)\mid f(x_1,\cdots,x_n)\in P[x_1,\cdots,x_n]\}.$$

所以，$P[a_1,\cdots,a_n]$ 的分式域

$$D(a_1,\cdots,a_n)=\{f(a_1,\cdots,a_n)g(a_1,\cdots,a_n)^{-1}\mid f,g\in P[x_1,\cdots,x_n],\ g(a_1,\cdots,a_n)\neq 0\},$$

必包含在每个含 $a_1,\cdots,a_n$ 的子域中，它就是由 $a_1,\cdots,a_n$ 在 F 中生成的子域，即

$$D(a_1,\cdots,a_n)=P(a_1,\cdots,a_n). \qquad \blacksquare$$

习 题 一

1. 仿照命题1证明中的方法，设 F 是个域，E 是 F 的一个扩域，$a\in E$，规定

$$\varphi: f(x)\to f(a),$$

则得 $F[x]$ 到 E 的一个环同态. 在下列情形，求出 $\mathrm{Ker}(\varphi)$ 的生成元（因为 $F[x]$ 是主理想环，核 $\mathrm{Ker}(\varphi)$ 是 $F[x]$ 的理想，从而必由某多项式生成）.

(a) $F=\mathbf{Q},\quad E=\mathbf{Q},\quad a=0$;

(b) $F=\mathbf{Q},\quad E=\mathbf{Q},\quad a=3$;

(c) $F=\mathbf{Q},\quad E=\mathbf{R},\quad a=\sqrt{2}$;

(d) $F=\mathbf{R},\quad E=\mathbf{C},\quad a=\mathrm{i}$;

(e) $F=\mathbf{R},\quad E=\mathbf{C},\quad a=-\mathrm{i}$.

2. 设 E 是域 F 的扩域，$a\in E$. 那么，F 和 a 在 E 中生成的子环 $F[a]$ 等于 F 和 a 在 E 中生成的子域 $F(a)$ 的充分必要条件是 a 为 F 上的代数元.

3. 证明：$\mathbf{Q}(\sqrt{2},\sqrt[3]{2})$ 是 $\mathbf{Q}$ 的单纯扩张.

§2 有限扩张

比单纯代数扩张略复杂，本节将讨论域的有限扩张.

熟悉一般域上向量空间理论的读者会发现，这里给出的某些新概念与向量空间理论中一些重要概念是一致的.

为了不加重那些没接触过一般域上线性代数学的读者的额外负担，也使本书能自成系统，不节外生枝，我们还是不采取从外书引用概念的办法.

定义1 设 E 是域 F 的扩张域. 说 E 中元素 $u_1,u_2,\cdots,u_n$ 是在 F 上**线性相关**的，如果有 $a_1,a_2,\cdots,a_n\in F$ 使得

(1) $a_1, a_2, \cdots, a_n$ 不全为 0；

(2) $a_1u_1 + a_2u_2 + \cdots + a_nu_n = 0$.

如果 $u_1, u_2, \cdots, u_n$ 在 F 上不是线性相关的，则说它们是在 F 上线性无关的.

例如，实数域 $\mathbf{R}$ 中的 $1, 2+\sqrt{5}$ 和 $2-\sqrt{5}$ 在有理数域 $\mathbf{Q}$ 上是线性相关的. 我们取 $a_1 = 1/4$, $a_2 = 1/4$, $a_3 = -1$，它们不全为 0，但

$$-1\cdot 1 + \frac{1}{4}(2+\sqrt{5}) + \frac{1}{4}(2-\sqrt{5}) = 0.$$

命题 1 设 E 是域 F 的一个扩张域. 如果 $a \in E$ 是 F 上的代数元，那么必有一个正整数 n 使得 E 中元

$$1, a, a^2, \cdots, a^n$$

在 F 上线性相关. 反之亦然.

证明 如果 a 是 F 上的代数元，那么必有 F 上的非零多项式

$$f(x) = a_0 + a_1x + \cdots + a_nx^n, \quad a_n \neq 0$$

使得 $f(a) = 0$，也就是

$$a_0\cdot 1 + a_1a + a_2a^2 + \cdots + a_na^n = 0,$$

且 $a_n \neq 0$. 这说明 $1, a, \cdots, a^n$ 在 F 上是线性相关的.

反之，若有正整数 n 使得 $1, a, \cdots, a^n$ 在 F 上线性相关，即有不全为 0 的 $a_0, a_1, \cdots, a_n \in F$ 使得

$$a_0\cdot 1 + a_1a + \cdots + a_na^n = 0.$$

那么，$f(x) = a_0 + a_1x + \cdots + a_nx^n$ 就是 F 上非零多项式，而且

$$a_0\cdot 1 + a_1a + \cdots + a_na^n = f(a) = 0. \quad \blacksquare$$

为了应用方便，我们对"不是线性相关"的意思解释一下.

E 中元素 $u_1, \cdots, u_n$ 在 F 上线性相关是说，它们的关系不一般，能找到 F 中 n 个元素 $a_1, a_2, \cdots, a_n$ 使得以下两件事同时成立：

(1) $a_1, a_2, \cdots, a_n$ 不全为 0，

(2) $a_1u_1 + \cdots + a_nu_n = 0$.

那么,若称 $u_1,u_2,\cdots,u_n$ 是线性无关的,即指 $u_1,u_2,\cdots,u_n$ 不是线性相关的,就是说,对于 $u_1,u_2,\cdots,u_n$,找不到 F 中 n 个元素,能同时满足条件(1)和条件(2). 换言之,你任意取 F 中 n 个元素 $a_1,\cdots,a_n$ 都不能同时满足(1)和(2),又等价于说,任取 F 中的 n 个元素 $a_1,\cdots,a_n$ 只要它满足(1)就一定不满足(2),要满足条件(2)则必破坏条件(1).

因此,称 $u_1,u_2,\cdots,u_n$ 是在 F 上线性无关的,当且仅当,对任意 $a_1,a_2,\cdots,a_n$,如果(2)成立,即

$$a_1u_1+a_2u_2+\cdots+a_nu_n=0,$$

则(1)必不成立,即 $a_1,\cdots,a_n$ 必然全为 0.

这里要特别提醒第一次接触这类概念的读者,所谓条件(1)不成立,是说不能"不全为 0",也就是必须全都为 0.

但是所说条件(1)和条件(2)不能同时成立,绝不是说,有 $a_1,a_2,\cdots,a_n\in F$ 使

1° $a_1,a_2,\cdots,a_n$ 全为 0,

2° $a_1u_1+\cdots+a_nu_n=0$.

这种否定办法不对. 因为用上述说法套在任何 n 个元素 $u_1,\cdots,u_n$ 上都是对的,故这种说法毫无意义.

命题 2 设 E 是域 F 的一个扩张域. 元素 $a\in E$ 是 F 上的超越元,当且仅当,对任意正整数 n, E 中元 $1,a,\cdots,a^n$,在 F 上都是线性无关的.

分析 这实际上是把命题 1 的条件和结论对换成否定形式,由于命题 1 给的是充分必要条件,所以命题 2 自然是对的. 但是为了培养能力,我们还是给出直接证明.

证明 如果 a 是 E 上的超越元,那么,对任意 $n+1$ 个不全为 0 的 $a_0,a_1,\cdots,a_n$ 必有

$$a_0\cdot 1+a_1a+\cdots+a_na^n\neq 0,$$

因为 a 不满足非零多项式

$$f(x)=a_0+a_1x+\cdots+a_nx^n.$$

这说明 $a_0,a_1,\cdots,a_n$ 满足定义 1 中条件(1)时必不满足(2)，所以，$1,a,\cdots,a^n$ 在 F 上线性无关.

反之，若，对任意 n，元素 $1,a,\cdots,a^n$ 在 F 上都是线性无关的. 那么，只要 $a_0,\cdots,a_n\in F$ 不全为 0 (也就是

$$f(x)=a_0+a_1x+\cdots+a_nx^n$$

不为零多项式)，则 $a_0\cdot1+a_1a+\cdots+a_na^n\neq0$. 从而

$$f(a)=a_0\cdot1+a_1a+\cdots+a_na^n\neq0.$$

也就是说，a 是 F 上的超越元. ▌

例题 1 实数域 $\mathbf{R}$ 中的数 $\sqrt{2},\sqrt{5}$ 在有理数域 $\mathbf{Q}$ 上线性无关.

证明 用反证法. 若 $\sqrt{2},\sqrt{5}$ 在 $\mathbf{Q}$ 上线性相关，则必有 $r,s\in\mathbf{Q}$，它们不全为 0，且

$$r\sqrt{2}+s\sqrt{5}=0.$$

若 $r\neq0$，将上式两端乘 $\sqrt{5}$，得

$$r\sqrt{10}+s=0,\quad \sqrt{10}=-s/r,$$

矛盾. 同样，$s\neq0$ 时也导出矛盾. ▌

定义 2 设 E 是域 F 的扩张域. 对于 E 中元 $v,u_1,\cdots,u_n$，如果有 $a_1,\cdots,a_n\in F$ 使

$$v=a_1u_1+\cdots+a_nu_n,$$

则说 v 是 $u_1,u_2,\cdots,u_n$ 的一个**线性组合**.

设 $u_1,u_2,\cdots,u_n$ 是 E 中元素，如果

(1) $u_1,u_2,\cdots,u_n$ 是线性无关的；

(2) 任意 $v\in E$，v 必然是 $u_1,u_2,\cdots,u_n$ 的一个线性组合；

则说 $u_1,u_2,\cdots,u_n$ 是 E 在 F 上的一个**基底**.

例题 2 设 F 是个域，$p(x)$ 是 F 上的 n 次不可约多项式，$E=F[x]/(p(x))$. 那么，E 中元

$$1+(p(x)),\ x+(p(x)),\ \cdots,\ x^{n-1}+(p(x)) \qquad (*)$$

是 E 在 F 上的一个基底.

证明 第五章§4之命题6证明了,E 的每个元素 v 均可唯一的表为

$$v=c_0+c_1x+\cdots+c_{n-1}x^{n-1}+(p(x))$$

形式.也就是

$$v=c_0[1+(p(x))]+\cdots+c_{n-1}[x^{n-1}+(p(x))],$$

即 v 中元都是(*)元的线性组合.

另一方面,如果 $a_0,\cdots,a_{n-1}\in F$ 使

$$a_0[1+(p(x))]+\cdots+a_{n-1}[x^{n-1}+(p(x))]=(p(x)),$$

即

$$f(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}\in(p(x)),$$

这说明次数不超过 $n-1$ 的多项式 $f(x)$ 一定能被 n 次不可约多项式 $p(x)$ 整除,$f(x)$ 只能是零多项式,于是,必有

$$a_0=a_1=\cdots=a_{n-1}=0,$$

即(*)是线性无关的.从而,它是 E 在 F 上的一个基底. ▌

例题3 设 E 是域 F 的一个扩张域,$a\in E$ 是 F 上的超越元.那么,$F(a)$ 在 F 上没有任何有限个元素能成为它的一个基底.

证明 $F(a)$ 的元素必形如

$$f(a)g(a)^{-1},\quad g(a)\neq 0,$$

其中 $f(x),g(x)$ 是 F 上多项式.

任取 $F(a)$ 的元素

$$f_1(a)g_1(a)^{-1},\quad\cdots,\quad f_n(a)g_n(a)^{-1},\qquad(*)$$

设多项式 $g_1(x)g_2(x)\cdots g_n(x)$ 的次数为 m,而多项式

$$f_1(x)g_2(x)\cdots g_n(x),\quad\cdots,\quad g_1(x)\cdots g_{n-1}(x)f_n(x)$$

次数最高者为 l.那么,选取一个 t 次多项式 $f(x)$,只要 $t>0$,$m+t>l$,则 $f(a)$ 必然不是(*)元素的线性组合.若不然,设有 $a_1,a_2,\cdots,a_n\in F$ 使

$$f(a)=a_1f_1(a)g_1(a)^{-1}+\cdots+a_nf_n(a)g_n(a)^{-1}.$$

则

$$f(a)g_1(a)\cdots g_n(a)=a_1f_1(a)g_2(a)\cdots g_n(a)+\cdots$$
$$+a_ng_1(a)\cdots g_{n-1}(a)f_n(a),$$

从而，a 满足一个次数大于0的多项式

$$f(x)g_1(x)\cdots g_n(x)-a_1f(x)g_2(x)\cdots g_n(x)-a_ng_1(x)\cdots f_n(x),$$

矛盾. ▌

命题3 设 E 是域 F 的扩张域，$u_1,\cdots,u_m$ 是 E 在 F 上的一个基底，$v_1,\cdots,v_n$ 也是 E 在 F 上的一个基底. 那么，$m=n$.

证明 若 $m\neq n$，不妨设 $m>n$. 由于 $u_1,\cdots,u_m$ 是基底，$v_1,\cdots,v_n$ 必是它们的线性组合，设

$$\begin{cases} v_1=a_{11}u_1+\cdots+a_{1m}u_m, \\ v_2=a_{21}u_1+\cdots+a_{2m}u_m, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ v_n=a_{n1}u_1+\cdots+a_{nm}u_m. \end{cases} \tag{1}$$

同理，$u_1,\cdots,u_m$ 又应都是 $v_1,\cdots,v_n$ 的线性组合

$$\begin{cases} u_1=b_{11}v_1+\cdots+b_{1n}v_n, \\ u_2=b_{21}v_1+\cdots+b_{2n}v_n, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ u_m=b_{m1}v_1+\cdots+b_{mn}v_n. \end{cases} \tag{2}$$

把(1)代入(2)的第一个式子，得

$$\begin{aligned} u_1 &= b_{11}(a_{11}u_1+\cdots+a_{1m}u_m) \\ &\quad +b_{12}(a_{21}u_1+\cdots+a_{2m}u_m) \\ &\quad +\cdots \\ &\quad +b_{1n}(a_{n1}u_1+\cdots+a_{nm}u_m) \\ &= \left(\sum_{i=1}^{n}b_{1i}a_{i1}\right)u_1+\cdots+\left(\sum_{i=1}^{n}b_{1i}a_{im}\right)u_m. \end{aligned}$$

从而

$$\left(1-\sum_{i=1}^{n} b_{1i}a_{i1}\right)u_1+\cdots+\left(\sum_{i=1}^{n} b_{1i}a_{im}\right)u_m=0.$$

而 $u_1,\cdots,u_m$ 线性无关,所以

$$\sum_{i=1}^{n} b_{1i}a_{i1}=1,\quad \sum_{i=1}^{n} b_{1i}a_{i2}=0,\quad \cdots,\quad \sum_{i=1}^{n} b_{1i}a_{im}=0.$$

把(1)分别代入(2)的第二个式子……就得到

$$\sum_{i=1}^{n} b_{2i}a_{i1}=0,\quad \sum_{i=1}^{n} b_{2i}a_{i2}=1,\quad \cdots,\quad \sum_{i=1}^{n} b_{2i}a_{im}=0,$$

$$\cdots,$$

$$\sum_{i=1}^{n} b_{mi}a_{i1}=0,\quad \sum_{i=1}^{n} b_{mi}a_{i2}=0,\quad \cdots,\quad \sum_{i=1}^{n} b_{mi}a_{im}=1.$$

这就是说,域 F 上的 $m\times m$ 阶矩阵

$$B=\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} & 0 & \cdots & 0\\ b_{21} & b_{22} & \cdots & b_{2n} & 0 & \cdots & 0\\ \vdots & \vdots & & \vdots & \vdots & & \vdots\\ b_{m1} & b_{m2} & \cdots & b_{mn} & 0 & \cdots & 0 \end{pmatrix}$$

与

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m}\\ \vdots & \vdots & & \vdots\\ a_{n1} & a_{n2} & \cdots & a_{nm}\\ 0 & 0 & \cdots & 0\\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

的乘积 BA 是 $m\times m$ 阶单位矩阵.

但是,取 F 上 $m\times m$ 阶矩阵

$$C=\begin{pmatrix} 0 & 0 & \cdots & 0\\ \vdots & \vdots & & \vdots\\ 0 & 0 & \cdots & 0\\ 0 & 0 & \cdots & 1 \end{pmatrix},$$

则显然有 $CB=0$.导致

$$C=CI=C(BA)=(CB)A=0A=0,$$

矛盾.所以,$m = n$. ▌

定义3 设E是域F的扩张域.如果E在F上有基底,则说E是F的一个**有限扩张**,基底所含元素的个数(这是由E和F唯一确定的一个正整数)称为E在F上的**扩张次数**,记为$[E:F]$.

例如,复数域$\mathbf{C}$在实数域$\mathbf{R}$上,元素1和$i=\sqrt{-1}$是个基底,从而$[\mathbf{C}:\mathbf{R}]=2$.

例题2中,$[E:F]]=n=\deg(p(x))$.

例题3中,a为F上超越元,$F(a)$不是F上的有限扩张.这种情形有时记为$[F(a):F]=\infty$.

定理1 设E是域F的有限扩张域,D是域E的有限扩张域.那么,D必为F的有限扩张,而且

$$[D:F]=[D:E][E:F].$$

证明 设$[D:E]=m$, $[E:F]=n$, $u_1,u_2,\cdots,u_m$是D在E上的一个基底,而$v_1,v_2,\cdots,v_n$是E在F上的一个基底.由于$E\subseteq D$,所以

$$u_1v_1,u_1v_2,\cdots,u_1v_n,\cdots,u_mv_1,\cdots,u_mv_n \tag{3}$$

都是D中元素.现断言,上记mn个D中元恰好是D在F上的一个基底.

对任意$a_{ij}\in F$ $(i=1,\cdots,m;\ j=1,2,\cdots,n)$,如果

$$\sum_{i=1,j=1}^{i=m,j=n} a_{ij}(u_iv_j)=0, \tag{4}$$

那么,每个$\sum_{j=1}^{n} a_{ij}v_j\,(i=1,2,\cdots,m)$都是$E$中元素,把它们分别记为$e_i$,则(4)式变成

$$\sum_{i=1}^{m} e_iu_i=0,\quad e_i\in E,\ i=1,2,\cdots,m.$$

但是$u_1,\cdots,u_m$是D在E上的基底,它们在E上线性无关,从而$e_1,\cdots,e_m$全都为0,即得到

$$\sum_{j=1}^{n} a_{ij} v_j = 0, \quad i = 1,2,\cdots,m.$$

注意这 m 个等式，每一个都是 E 在 F 上的基底 $v_1,\cdots,v_n$ 的线性组合等于 0，从而

$$a_{11} = a_{12} = \cdots = a_{1n} = 0,$$
$$a_{21} = a_{22} = \cdots = a_{2n} = 0,$$
$$\cdots,$$
$$a_{m1} = a_{m2} = \cdots = a_{mn} = 0.$$

即(3)这组向量在 F 上线性无关.

进一步，任取 D 中元素 b. 由于 $u_1,\cdots,u_m$ 是 D 在 E 上的基底，b 必为它们的一个线性组合，即有 $a_1,\cdots,a_m \in E$ 使得

$$b = a_1u_1 + a_2u_2 + \cdots + a_mu_m. \tag{5}$$

但是，$v_1,\cdots,v_n$ 是 E 在 F 上的一个基底，从而每个 a_i 都是它们的一个线性组合，即有 $a_{ij} \in F$ 使得

$$a_i = \sum_{j=1}^{n} a_{ij} v_j, \quad i = 1,2,\cdots,m \tag{6}$$

把(6)式代到(5)中去，得

$$b = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}(u_i v_j).$$

这说明 D 的每一个元素都是元素组(3)的一个线性组合. 从而(3)是 D 在 F 上的一个基底. 而且

$$[D:F] = mn = [D:E][E:F].$$ ▌

命题 4 设 E 是 F 的一个扩张域，E 中元 $u_1,\cdots,u_n$ 在 F 上线性无关，v 是 $u_1,\cdots,u_n$ 的一个线性组合

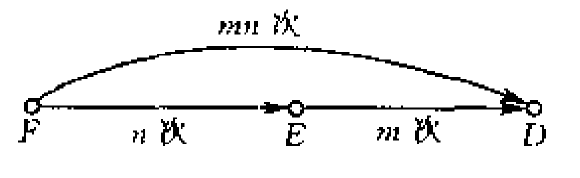


图 7-1

$$v = a_1u_1 + a_2u_2 + \cdots + a_nu_n, \quad a_i \in F. \tag{7}$$

那么，这种表法是唯一的.

证明 假设还有 $b_1,\cdots,b_n\in F$ 使

$$v=b_1u_1+b_2u_2+\cdots+b_nu_n. \tag{8}$$

那么，将(7),(8)两式相减，得

$$(a_1-b_1)u_1+\cdots+(a_n-b_n)u_n=0.$$

由于 $u_1,\cdots,u_n$ 线性无关，故必有

$$a_1-b_1=a_2-b_2=\cdots=a_n-b_n=0,$$

即 $a_1=b_1,\ \cdots,\ a_n=b_n$. ▎

命题 5 设 E 是 F 的一个有限扩张，$u_1,\cdots,u_n$ 是 E 在 F 上的一个基底.如果表示

$$v=a_1u_1+a_2u_2+\cdots+a_nu_n,\quad a_i\in F \tag{9}$$

中，$a_1\neq0$，则 $v,u_2,\cdots,u_n$ 也是 E 在 F 上的一个基底.

证明 首先，用于 $a_1\neq0$，故

$$a_1u_1=v-a_2u_2-\cdots-a_nu_n,$$
$$u_1=a_1^{-1}v-(a_1^{-1}a_2)u_2-\cdots-(a_1^{-1}a_n)u_n,$$

即 u_1，是 $v,u_2,\cdots,u_n$ 的线性组合.

因为 $u_1,u_2,\cdots,u_n$ 是个基底，E 中每个元均可是它们的线性组合，而 u_1 又是 $v,u_2,\cdots,u_n$ 的线性组合，故 E 之每个元素均为 $v,u_2,\cdots,u_n$ 的一个线性组合.

如果 $v,u_2,\cdots,u_n$ 线性相关，即有不全为 0 的 $b_1,b_2,\cdots,b_n\in F$，使得

$$b_1v+b_2u_2+\cdots+b_nu_n=0. \tag{10}$$

当 $b_1=0$ 时，$b_2,\cdots,b_n$ 不全为 0，(10)式意味着 $u_2,\cdots,u_n$ 线性相关，矛盾.当 $b_1\neq0$ 时，有

$$v=(-b_1^{-1}b_2)u_2+\cdots+(-b_1^{-1}b_n)u_n,$$

得到等式与(9)式不同，(9)中 $a_1\neq0$.但命题 4 已证明了表法唯一性，又得一矛盾.

所以，$v, u_2, \cdots, u_n$ 还是线性无关的，从而它们是 E 在 F 上的一个基底. ▌

命题 6 设 E 是域 F 的一个有限扩张域. $u_1, u_2, \cdots, u_m$ 是 E 在 F 上的一个基底，$v_1, \cdots, v_k$ 是 E 中 k 个在 F 上线性无关的元素，那么，可将 $u_1, u_2, \cdots, u_m$ 替除 k 个，剩下 $u_{i_1}, \cdots, u_{i_{n-k}}$ 使

$$v_1 v_2, \cdots, v_k, u_{i_1}, \cdots, u_{i_{n-k}}$$

是 E 在 F 上的一个基底.

证明 由于 $v_1, \cdots, v_k$ 线性无关，故 $v_1 \neq 0$,

$$v_1 = a_1 u_1 + \cdots + a_n u_n, \quad a_i \in F,$$

其中之诸 a_i 至少有 1 个不为 0，比方说 $a_1 \neq 0$. 那么，由命题 5，知 $v_1, u_2, \cdots, u_n$ 为 E 的一个基底.

这样，v_2 必为 $v_1, u_2, \cdots, u_n$ 的线性组合，

$$v_2 = b_1 v_1 + b_2 u_2 + \cdots + b_n u_n,$$

且 $b_2, \cdots, b_n$ 至少有一个不为 0. 否则出现

$$v_2 = b_1 v_1, \quad -v_2 + b_1 v_1 = 0$$

与 $v_1, \cdots, v_k$ 线性无关之假定相矛盾. 不妨设 $b_2 \neq 0$. 于是，由命题 5，知 $v_1, v_2, u_3, \cdots, u_n$ 为 E 的一个基底.

一直做下去，即得所要结论. ▌

推论 设 E 是 F 的有限扩张，$[E:F] = n$. 那么，E 中任意 $n+1$ 个元素恒线性相关. ▌

定理 2 设 D, E, F 都是域，$F \subseteq E \subseteq D$，且 D 是 F 的有限扩张. 则 E 是 F 的有限扩张，而且 $[E:F] \mid [D:F]$.

证明 任取 $v_1 \in E$, $v_1 \neq 0$，那么 v_1 一个元素在 F 上是线性无关的. 如果任取 $v \in E$, v, v_1 都是线性相关的，即有 $a, b \in F$, a, b 不全为 0，且

$$av + bv_1 = 0.$$

则 $a \neq 0$，否则 $bv_1 = 0$, $b \neq 0$，矛盾. 从而有

$$v = -(a^{-1}b)v_1,$$

即每个 v 都是 v_1 的线性组合.

v_1 即是 E 在 F 上的一个基底.

如果有 $v_2 \in E$,使 v_1, v_2 线性无关.再来看是否每个 $v \in E$ 都使得 v, v_1, v_2 都线性相关.是,则 v_1, v_2 为基底.否,则有 v_1, v_2, v_3 线性无关…….

由于 D 在 F 上至多有 n 个元素线性无关,此事不能无止无休.必止于某步,即有 $v_1, \cdots, v_m$ 成为 E 在 F 上的一个基底.

同样的方法施之于 E 的扩张 D.如果 $u_1, u_2, \cdots, u_l$ 是 D 在 E 上的线性无关的元素,那么

$$u_1v_1, \cdots, u_1v_m, \cdots, u_lv_1, \cdots, u_lv_m$$

必然是 D 在 F 上的线性无关元素,必有 $lm \leqslant n$,从而 l 不能无限地增大下去.

最后,得

$$u_1, u_2, \cdots, u_t \tag{11}$$

是 D 在 E 上线性无关的,且任意 $u \in D$ 均使

$$u, u_1, u_2, \cdots, u_t$$

线性相关(从而 u 必为 $u_1, \cdots, u_t$ 的线性组合).此时,(11)即为 D 在 E 上的一个基底.由定理 1 知 $tm = n$. ▌

命题 7 设 E 是域 F 的扩张域,$a, b \in E$ 是 F 上的代数元,其极小多项式分别是 m 次和 n 次的.那么 $F(a,b)$ 也是 F 上的有限扩张,且

$$[F(a,b):F] \leqslant mn.$$

证明 由§1之定理 2 的推论知

$$F(a)(b) = F(a,b).$$

再据定理 1,知 $F(a,b)$ 是 F 上的有限扩张,且

$$[F(a,b):F] = [F(a)(b):F(a)][F(a):F].$$

注意§1之例题 2,$[F(a):F] = m$.同时,若

$$g(x)=a_0+a_1x+\cdots+a_nx^n, \quad a_n\in F$$

是 b 在 F 上的极小多项式，那么 $g(b)=0$. 而 $g(x)$ 当然也是域 $F(a)$ 上的多项式，$g(b)=0$ 即意味着 b 在 $F(a)$ 上的极小多项式 $p(x)$ 必然整除 $g(x)$. 设 $\deg p(x)=t$，则

$$[F(a,b):F]=[F(a)(b):F(a)][F(a):F]=tn.$$

它当然不大于 mn. ∎

命题 7 可解释为如下图式.

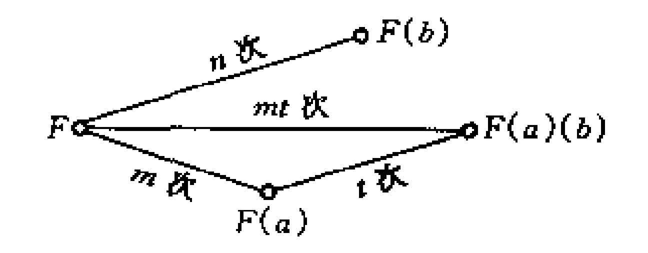


图 7-2

例题 4 计算 $[\mathbf{Q}(\sqrt{2}+\sqrt{3}):\mathbf{Q}]$.

解法 1 显然，$\mathbf{Q}(\sqrt{2}+\sqrt{3})\subseteq\mathbf{Q}(\sqrt{2})(\sqrt{3})$. 又 $\sqrt{2}$，$\sqrt{3}$ 分别以 x^2-2，x^2-3 为其在有理数域上的极小多项式. 故

$$[\mathbf{Q}(\sqrt{2}):\mathbf{Q}]=2, \quad [\mathbf{Q}(\sqrt{3}):\mathbf{Q}]=2.$$

由命题 7 可知

$$[\mathbf{Q}(\sqrt{2}+\sqrt{3}):\mathbf{Q}]\leqslant[\mathbf{Q}(\sqrt{2})(\sqrt{3}):Q]\leqslant 2\times 2=4.$$

从而 $\sqrt{2}+\sqrt{3}$ 在 $\mathbf{Q}$ 上的极小多项式次数要整除 4，只能是 2 或 4 次.

若有 2 次多项式为 $\sqrt{2}+\sqrt{3}$ 的一个极小多项式，则必有有理数 a,b,c 使

$$a(\sqrt{2}+\sqrt{3})^2+b(\sqrt{2}+\sqrt{3})+c=0, \quad a\neq 0. \tag{11}$$

从而

$$2a+3a+2a\sqrt{6}+b\sqrt{2}+b\sqrt{3}+c=0. \tag{12}$$

两端同乘 $\sqrt{2}$，得

$$2b+(5a+c)\sqrt{2}+4a\sqrt{3}+b\sqrt{6}=0. \tag{13}$$

将(13)乘 $2a$ 减去(12)乘 b，得

$$4ab-b(5a+c)+(2a(5a+c)-b^2)\sqrt{2}+(8a^2-b^2)\sqrt{3}=0, \tag{14}$$

$$-(8a^2-b^2)\sqrt{3}=4ab-b(5a+c)+[2a(5a+c)-b^2]\sqrt{2}.$$

将上式两端再平方,其余各项均为有理数.故$\sqrt{2}$前的系数必为 0,即

$$2a(5a+c)-b^2=0. \tag{15}$$

再看(14)式,$8a^2-b^2$ 必为 0,否则$\sqrt{3}$为有理数,矛盾.再进一步,更可得到(仍由(14)),

$$4ab-b(5a+c)=0. \tag{16}$$

将(15)乘 b 加到(16)乘 $2a$ 上,得

$$8a^2b-b^3=(8a^2-b^2)b=0.$$

若 $b=0$,由(11)立即推出 $a=c=0$,矛盾.

若 $8a^2-b^2=0$,而 a 和 b 都是有理数,亦为矛盾.

所以,$\sqrt{2}+\sqrt{3}$在 $\mathbf{Q}$ 上的极小多项式必然是 4 次的,

$$[\mathbf{Q}(\sqrt{2}+\sqrt{3}):\mathbf{Q}]=4.$$

解法 2 一方面,显然有 $\mathbf{Q}(\sqrt{2}+\sqrt{3})\subseteq\mathbf{Q}(\sqrt{2},\sqrt{3})$.另一方面,在实数域中,有

$$\sqrt{3}-\sqrt{2}=(\sqrt{3}+\sqrt{2})^{-1}\in\mathbf{Q}(\sqrt{3}+\sqrt{2}).$$

所以

$$\sqrt{3}=\frac{1}{2}(\sqrt{3}-\sqrt{2})+\frac{1}{2}(\sqrt{3}+\sqrt{2})\in\mathbf{Q}(\sqrt{3}+\sqrt{2}).$$

同理$\sqrt{2}\in\mathbf{Q}(\sqrt{2}+\sqrt{3})$.所以,

$$\mathbf{Q}(\sqrt{2}+\sqrt{3})=\mathbf{Q}(\sqrt{2},\sqrt{3}).$$

看$\sqrt{3}$在 $\mathbf{Q}(\sqrt{2})$上的极小多项式.现断言$\sqrt{3}$不是 $\mathbf{Q}(\sqrt{2})$中元素.否则,设有有理数 r,s 使

$$\sqrt{3}=r\sqrt{2}+s,$$

两端平方得 $3+2r^2+s^2=2r\sqrt{2}$,必有 $r=0$,进而 $s=\sqrt{3}$,矛盾.

由于$\sqrt{3}$在 $\mathbf{Q}$ 上极小多项式是 2 次的，它在 $\mathbf{Q}(\sqrt{2})$上极小多项式只能是 2 次的，所以

$$[\mathbf{Q}(\sqrt{2}+\sqrt{3}):\mathbf{Q}]=[\mathbf{Q}(\sqrt{2})(\sqrt{3}):\mathbf{Q}(\sqrt{2})]$$
$$[\mathbf{Q}(\sqrt{2}):\mathbf{Q}]=2\times 2=4.$$

解法 1 证明 $1,\sqrt{2},\sqrt{3},\sqrt{6}$在 $\mathbf{Q}$ 上线性无关这一事实比较费事. ∎

例题 5 设 F 是个域，$f(x)$和 $g(x)$都是 F 上的不可约多项式，

$$\deg(f(x))=m,\quad \deg(g(x))=n.$$

E 为 F 的扩张域，$a\in E$，$g(a)=0$. 证明：当 m,n 互素时，$f(x)$必然在域 $F(a)$上也是不可约多项式.

证明 作域 F 的单纯代数扩张 $F(b)$，使得 b 满足 F 上多项式 $f(x)$.

由§1 定理 2 的推论知

$$F(a,b)=F(a)(b)=F(b)(a).$$

再由命题 7 知，当$[F(a):F]=\deg(g(x))=n$ 时，

$$[F(a)(b):F]=nt\leqslant nm.$$

同理，由于$[F(b):F]=\deg(f(x))=m$，故

$$[F(b)(a):F]=ms\leqslant mn.$$

于是，由 $nt=ms$ 知 $n\mid(ms)$. 另一方面，m,n 互素，必有整数 k,l 使

$$mk+nl=1,$$
$$smk+snl=s,$$
$$ntk+snl=s,$$

这导致 $n\mid s$. 而 $s\leqslant n$，从而必有 $s=n$.

这说明$[F(a,b):F]=[F(a)(b):F(a)][F(a):F]=mn$. 所以，$F(a)(b)$在 $F(a)$上是 m 次扩张.

再进一步，又说明 b 满足$F(a)$上 m 次不可约多项式，可设为 $p(x)$.

由于 $f(x)$ 也是 $F(a)$ 上多项式，且 $f(b)=0$，而 $p(x)$ 是 b 在 $F(a)$ 上的极小多项式，故

$$p(x) \mid f(x),$$

且 $p(x)$ 与 $f(x)$ 次数相同，它们必然是相伴的. 所以，$f(x)$ 在 $F(a)$ 上也是不可约的. ▌

下面的例题可以帮助读者复习一些概念.

例题 6 设 F 是个有 8 个元素的域，讨论 F 的结构.

解 $8=2^3$，F 的素域（极小域）只能含 2 个元素（F 的特征数必为 2）.

设 $P=\{0^*, 1^*\}$ 是 F 的素域，在同构的观点下可以认为 $P=\mathbf{I}_2$.

由于 F 是有限的，F 必为域 P 的有限扩张. 任取 $a \in F$，$a \notin P$，则 a 必为 P 上的代数元. 设 $f(x) \in \mathbf{I}_2[x]$ 是 a 在 $\mathbf{I}_2$ 上的极小多项式.

因为 $\mathbf{I}_2(a)$ 是 F 的子域，所以 $\mathbf{I}_2(a)$ 也是 $\mathbf{I}_2$ 的有限扩张. 且

$$[\mathbf{I}_2(a):\mathbf{I}_2] \mid [F:\mathbf{I}_2]=3. \qquad (*)$$

这里让我们解释一下是怎样知道 $[F:\mathbf{I}_2]$ 等于 3 的. 事实上，$[F:\mathbf{I}_2]$ 有限，如果 $u_1, \cdots, u_n \in F$ 是 F 在 $\mathbf{I}_2$ 上的基底，则

$$F=\{\alpha_1 u_1+\cdots+\alpha_n u_n \mid \alpha_i \in \mathbf{I}_2\},$$

对于 F 中的一个元素，$\alpha_1, \cdots, \alpha_n$ 是唯一确定的（表法唯一所致），而 $\alpha_i \in \mathbf{I}_2$ 只有两个可能，所以 F 有 2^n 个不同的元素. 但已知 $2^n=8$，故推知 $n=3$.

由于 $a \notin \mathbf{I}_2$，$(*)$ 意味着 $[\mathbf{I}_2(a):\mathbf{I}_2]=3$，也就是说 $\mathbf{I}_2(a)$ 在 $\mathbf{I}_2$ 上的次数为 3，而这个次数又等于 a 在 $\mathbf{I}_2$ 上的极小多项式 $f(x)$ 的次数.

$\mathbf{I}_2$ 上的 3 次多项式只有

$$x^3+x^2, \qquad x^3+x+1^*,$$

$$x^3+x^2+x, \qquad x^3+1^*,$$

$$x^3+x^2+x+1^*, \qquad x^3,$$
$$x^3+x^2+1^*, \qquad x^2+x,$$
其中只有 x^3+x+1^* 和 $x^3+x^2+1^*$ 既不以 0^* 也不以 1^* 为根，它们不能被 1 次多项式整除，从而是 $\mathbf{I}_2$ 上不可约多项式.

若 a 的极小多项式 $f(x)=x^3+x^2+1$，那么
$$a^3+a^2+1=0.$$
从而有（注意，特征数为 2，$a+a=0^*$）
$$(a^3+a^2+a+1^*)+(a+1^*)+1^*=0,$$
也就是 $a+1^*$ 满足不可约多项式 x^3+x+1. 而 $\mathbf{I}_2(a+1)$ 也等于 F. 可以把 a 为生成元的一切讨论结果都移到以 $a+1^*$ 为生成元的情形.

所以，现在可设直接假定 a 满足不可约多项式 $f(x)=x^3+x+1^*$. 于是知道 F 的 8 个元素是 $0^*,1^*,a,a+1^*,a^2,a^2+1,a^2+a+1,a^2+a$，其中 a 满足 $a^3+a^2+1^*=0^*$（即 $a^3=a^2+1^*$）.

域 F 有 8 个元素，那么 $F-\{0^*\}$ 是个 7 元乘法群，7 是素数，$F-\{0^*\}$ 是个循环群，而且除恒等元外都是生成元. 计算之，得
$$a, a^2, \quad a^3=a+1^*, \quad a^4=a^2+a,$$
$$a^5=a^2+a+1^*, \quad a^6=a^2+1^*, \quad a^7=1^*.$$

这样，F 的乘法表就十分清楚了.

至于 F 的加法，注意到其特征数为 2，也就一下子都可以写出来了. ▎

习 题 二

1. 证明：$\mathbf{Q}(\sqrt{2},\mathrm{i})$ 是 $\mathbf{Q}$ 的单纯扩张，又是 $\mathbf{Q}$ 的有限扩张并给出 $\mathbf{Q}(\sqrt{2},\mathrm{i})$ 在 $\mathbf{Q}$ 上的一组基底.

2. 设 K 是域 F 的一个有限扩张域，$[K:F]=p$，其中 p 是个素数. 那么 K 必为 F 的一个单纯扩张.

3. 设 K 是域 F 的一个有限扩张域，$[K:F]=n$，而 $f(x)$ 是 F 上的不可约多项式，$\deg(f(x))=m$. 如果 m 和 n 互素，那么作为 K 上多项式的

$f(x)$在 K 中没有根.

4. 求 $\mathbf{Q}(\sqrt{2+\sqrt{3}})$在 $\mathbf{Q}$ 上的扩张次数$[\mathbf{Q}(\sqrt{2+\sqrt{3}}):\mathbf{Q}]$.

§3 代数扩张

比有限扩张更广泛一些,本节讨论域的代数扩张.

定义 1 设 E 是域 F 的一个扩张域. 如果任意 $a\in E$ 都是 F 上代数元,则说 E 是 F 的一个**代数扩张域**或**代数扩张**.

例 1 复数域 $\mathbf{C}$ 是实数域 $\mathbf{R}$ 的一个代数扩张. 因为,对任意 $a\in\mathbf{C}$,如果 $a\in\mathbf{R}$,那么它满足 $\mathbf{R}$ 上多项式

$$x-a,$$

a 当然为 F 上代数元;如果 $a\in\mathbf{C}$, $a\in\mathbf{R}$,则

$$a=b+\mathrm{i}c,\quad b,\ c\in\mathbf{R},\ c\neq 0.$$

它满足 $\mathbf{R}$ 上的二次多项式

$$x^2-2bx+(b^2+c^2),$$

a 亦为 F 上的代数元.

例 2 实数域 $\mathbf{R}$ 不是有理数域 $\mathbf{Q}$ 的代数扩张. 人们已经证明了,实数 π(圆周率),e(自然对数底)和 $2^{\sqrt{2}}$ 等都不能满足任何有理多项式.

命题 1 如果 E 是域 F 的有限扩张,那么它一定是 F 的一个代数扩张.

证明 设$[E:F]=n$. 任取 $a\in E$,据§2 命题 6 之推论,E 中的下列 $n+1$ 个元素

$$1,a,a^2,\cdots,a^n$$

必然在 F 上线性相关,即有不全为 0 的数 $a_0,a_1,\cdots,a_n\in F$ 使

$$a_0+a_1a+\cdots+a_na^n=0;$$

也就是 a 满足 F 上非 0 多项式

$$f(x)=a_0+a_1x+\cdots+a_nx^n.$$

a 为 F 上的代数元. ∎

至此，很容易产生这样的疑问，代数扩张是否也必为有限扩张呢？回答是否定的.

命题 2 设 E 是域 F 的一个扩张域. 如果 $a,b\in E$ 都是 F 上的代数元，那么 $a+b,a-b,ab$ 都是 F 上代数元；当 $b\neq 0$ 时，ab^{-1} 也是域 F 上的代数元.

证明 设 $a,b\in E$ 是 F 上的代数元. 由 §2 命题 7 知，$F(a,b)$ 也是 F 上的有限扩张，再由命题 1 知，$F(a,b)$ 是 F 上的代数扩张. 从而 $F(a,b)$ 的每个元素都是 F 上代数元.

由于 $a,b\in F(a,b)$，故元素

$$a+b,a-b,ab\in F(a,b),$$

它们都是 F 上代数元. 当 $b\neq 0$ 时，$ab^{-1}\in F(a,b)$，它亦为 F 上之代数元. ▌

命题 3 设 E 是域 F 的一个扩张域. 那么

$$G=\{a\in E\mid a \text{ 是} F \text{ 上代数元}\}$$

是 E 的一个子域，G 是 F 的一个代数扩张域.

证明 因为 $F\subseteq G$，命题 3 就是命题 2 的直接推论. ▌

例题 1 令 $G=\{a\in\mathbf{C}\mid a$ 是 $\mathbf{Q}$ 上代数元$\}$. 那么，G 不是 $\mathbf{Q}$ 上的有限扩张.

分析 用反证法. 设 $[G:\mathbf{Q}]=t$. 我们只要能找到 $\mathbf{Q}$ 上一个不可约多项式 $p(x)$，

$$\deg(p(x))=r>t,$$

由代数基本定理知道必有 $a\in\mathbf{C}$，使 $p(a)=0$，但是

$$\mathbf{Q}(a)\cong\mathbf{Q}[x]/(p(x)),$$

$$[\mathbf{Q}(a):\mathbf{Q}]=r>t=[G:\mathbf{Q}],$$

同时，a 是 $\mathbf{Q}$ 上代数元，$\mathbf{Q}(a)\subseteq G$，此为矛盾.

证明 设 $[G:\mathbf{Q}]=t$. 取一素数 $p>t+1$. 看整数环 $\mathbf{I}$ 上的多项式

$$f(x)=x^{p-1}+px^{p-2}+p(p-1)x^{p-3}+\cdots+p(p-1)x+p.$$

如果它是可约的，± 1 不计，它必可写成形如

$$g(x)=1+c_1x+\cdots+c_{m-1}x^{m-1}+x^m,\quad m<p-1,$$
$$h(x)=p+b_1x+\cdots+b_{n-1}x^{n-1}+x^n,\quad n<p-1$$

的两个多项式之积,否则首系数不为 1 或常数项不为素数 p.

注意对 $b_1,\cdots,b_{n-1}$,不妨假设 $b_1,\cdots,b_{i-1}$ 能被 p 整除,而 $p\nmid b_i$.

比较 $f(x)=g(x)h(x)$ 两端 i 次项系数,右端 $g(x)h(x)$ 之 x^i 前系数应为

$$b=b_i+b_{i-1}c_1+b_{i-2}c_2+\cdots+pc_i,$$

由于 $p\mid b_{i-1}$, $p\mid b_{i-2}$, $\cdots$,所以,p 可整除上式右端除 b_i 外其余每项,从而 $p\nmid b$.

但 $f(x)$ 之 x^i 系数能被 p 整除,得一矛盾. $f(x)$ 是 **I** 上不可约多项式,从而必为 **Q** 上不可约多项式.

设 $a\in\mathbf{C}$, $f(a)=0$,则

$$[\mathbf{Q}(a):\mathbf{Q}]=p-1,$$
$$[G:\mathbf{Q}]\geqslant[\mathbf{Q}(a):\mathbf{Q}]=p-1>t,$$

矛盾. ▎

这个例题告诉我们,代数扩张和有限扩张不是等价概念.其包含关系是

$$\{单纯代数扩张\}<\{有限扩张\}<\{代数扩张\}.$$

定理 1 设 D,E,F 都是域,而且 E 是 F 的代数扩张,D 是 E 的代数扩张.那么,D 也是 F 的代数扩张.

证明 任取 $a\in D$.据定义,有非零多项式 $p(x)\in E[x]$,

$$p(x)=c_0+c_1x+\cdots+c_nx^n,\quad c_i\in E,$$

使得 $p(a)=0$.

由于 $c_0,c_1,\cdots,c_n\in E$, E 是 F 的代数扩张,故可设

$$[F(c_i):F]=m_i,\quad i=0,1,\cdots n.$$

由 §1 定理 2 的推论和 §2 定理 1,知

$$H=F(c_0,c_1,\cdots,c_n)=F(c_0)(c_1)\cdots(c_n)$$

是 F 的有限扩张，次数不大于 $m_0 m_1 \cdots m_n$.

再由

$$a \in H(a) = F(c_0, \cdots, c_n)(a),$$

而 $F(c_0, \cdots, c_n)(a)$ 也是 F 的有限扩张（§2 定理 1），进而它是 F 的代数扩张，a 为 F 上的代数元. ▌

例题 2 设 D 是域 F 的一个代数扩张域，R 是 D 的子环，且 $F \subseteq R \subseteq D$. 那么，$R$ 必为 D 的子域.

证法 1 对任意 $a \in R$，如果 $a \neq 0$，且 $a \notin F$，由于 a 是 F 上代数元，必有 F 上不可约多项式

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n, \quad a_n \neq 0, \ n > 1$$

使得 $p(a) = 0$.

$p(x)$ 不可约蕴涵着 $a_0 \neq 0$，否则必有

$$p(x) = x(a_1 + a_2 x + \cdots + a_n x^{n-1}).$$

于是，

$$-a_0^{-1}(a_n a^n + \cdots + a_1 a) = 1,$$

$$-a_0^{-1}(a_n a^{n-1} + \cdots + a_1) a = 1.$$

这说明

$$a^{-1} = (-a_0^{-1} a_n) a^{n-1} + \cdots + (-a_0^{-1} a_1),$$

而 R 是个子环，$a \in R$，$F \subseteq R$，故

$$a^{-1} = (-a_0^{-1} a_n) a^{n-1} + \cdots + (-a_0^{-1} a_1) \in R.$$

R 之每个非零元恒有逆，R 为域.

证法 2 对任意 $a \in R$，$a \neq 0$，由于 a 是 F 上的代数元，$F(a)$ 是 F 上的单纯代数扩张，$F(a)$ 是个域，$a^{-1} \in F(a)$. 从而有 $a_1, \cdots, a_n \in F$ 使

$$a^{-1} = a_1 + a_2 a + \cdots + a_n a^{n-1},$$

显然，$a^{-1} \in R$. R 是 D 的子域. ▌

例题 2 说明域的单纯代数扩张、有限扩张和代数扩张不是等价概念. 但是，对有些域来说，它的单纯代数扩张和有限扩张是一

回事. 下面,我们来证明,素域

$$\mathrm{I}_p=\{0^*,1^*,\cdots,(p-1)^*\},\quad p \text{ 是素数}$$

的任意有限扩张域,必为其上的单纯代数扩张域.

域只含有限个元素时称为**有限域**.

命题 4 设 F 是个有限域,P 是 F 的素域. 那么 F 必为 P 的有限扩张. 设 $[F:P]=n$,则 F 的元数恰好是 p^n,其中 p 是 P 的元数.

证明 因为 F 的元数有限,它只能有有限个不同的在 P 上线性无关的元素组. 设 P 上线性无关的元素组

$$u_1,u_2,\cdots,u_n$$

在各线性无关元素组中是元数最多的一个.

此时,任取 $v\in F$,元素 $v,u_1,\cdots,u_n$ 必然是在 P 上线性相关的,进而 v 必为 $u_1,\cdots,u_n$ 的一个线性组合. 这说明,$u_1,\cdots,u_n$ 就是 F 在 P 上的一个基底. $[F:P]=n$.

由于 F 中的元素恒可唯一地表为

$$a_1u_1+a_2u_2+\cdots+a_nu_n,\quad a_i\in F,$$

而 a_1 有 p 个不同的选择,a_2 又有 p 个不同的选择,故有 p^n 个不同的表达式;也就是说,F 恰有 p^n 个元素. ▍

命题 5 任意有限域 F 必为其素域 P 的一个单纯代数扩张.

证明 设 P 有 p 个元素,p 必然是个素数. 再设 $[F:P]=n$. 则 F 有 p^n 个元素.

用 G 代表 F 的非零元的集合,因为 F 是个域,G 在 F 的乘法之下是个交换群. 且 $|G|=q=p^n-1$.

设群 G 中元素的阶数最大为 t,由第二章 §5 之定理 1 知 $t|q$.

另一方面,设 $a\in G$, a 的阶数为 t,

$$a^t=1.$$

即意味着,a 满足 P 上多项式

$$x^t-1.$$

但，t 是交换群G 中元素的最大阶数，由第二章§5之命题5知，G 的任意元 b 的阶数 s 都要整除 t，故 $b^s=1, b^t=1$.

这说明 G 之每个元都满足P 上多项式 x^t-1. 但域上 t 次多项式至多有 t 个不同的根，故又有 $q\leqslant t$.

所以，$q=t$，而 t 是a 的阶数

$$1, a, \cdots, a^{t-1}$$

是两两不同的 t 个元素，它们即为 G 之全部元素. G 是由 a 生成的循环群.

F 是由P 和a 生成的域，$F=P(a)$，F 是P 上单纯扩张. ▌

例题3 设 F 是个域，α 是F 上的一个超越元. 那么，域$F(\alpha)$ 中的元素

$$\beta=\alpha^3/(\alpha+1)$$

也是 F 上的超越元，但域 $F(\alpha)$是域 $F(\beta)$的单纯代数扩张.

证明 如果 β 是F 上的代数元，则必有 F 上多项式$f(x)=a_nx^n+\cdots+a_0$ 使得

$$f(\beta)=a_n\beta^n+\cdots+a_1\beta+a_0=0, \quad a_n\neq0.$$

从而有

$$a_n\left(\frac{\alpha^3}{\alpha+1}\right)^n+\cdots+a_1\left(\frac{\alpha^3}{\alpha+1}\right)+a_0=0.$$

两端同乘$(\alpha+1)^n$，又得

$$a_n\alpha^{3n}+\cdots+a_1\alpha^3(\alpha+1)^n+a_0(\alpha+1)^n=0,$$

这说明 α 满足一个F 上的 $3n$ 次的多项式，α 应该是F 上的代数元，矛盾.

再证元素 α 在域$F(\beta)$上，由于

$$\alpha^3-\beta\alpha-\beta=\alpha^3-(\alpha+1)\frac{\alpha^3}{\alpha+1}=0,$$

也就是 α 满足$F(\beta)$上的多项式

$$g(x)=x^3-\beta x-\beta,$$

所以 α 是$F(\beta)$的代数元. α 在$F(\beta)$上的极小多项式 $p(x)$要整除

$g(x)$，$p(x)$的次数只能是 3 次或 2 次．所以$[F(\alpha):F(\beta)]$有限，$F(\alpha)$的每个元素都是 $F(\beta)$上的代数元． ▮

习　题　三

1．设 E，G，K 都是域 F 的扩张域，且 $E\subseteq K$，$G\subseteq K$．证明：如果 E 是 F 的代数扩张，G 是 F 的代数扩张，那么 $G\cup E$ 在 K 中生成的子域 L 也是 F 的一个代数扩张．

2．设有限域 F 的特征数为 p．证明：

$$\sigma: a\to a^p,\quad a\in F$$

是 F 的一个自同构映射．进而说明，对任意 $b\in F$ 有唯一的一个元素 $c\in F$ 使得

$$c^p=b.$$

3．设 K 是域 F 的代数扩张，G 是 K 的扩张域，$a\in G$ 是 K 上的代数元．那么，a 必然是 F 上的代数元．

§4　代数封闭域

设 F 是个域．我们已经看到，F 上的一个单纯代数扩张 $E=F(a)$和 F 上的一个不可约多项式密切相连．如果 E 是 F 的一个真的扩张，即 $a\notin F$，那么对应的不可约多项式必然是次数不小于 2．

所以，若域 F 上没有次数不小于 2 的不可约多项式，那么，F 就没有真的单纯代数扩张，进而也就没有真的代数扩张．

例如，复数域上任意一个次数大于等于 2 的多项式都可以分解成一次多项式之积，n 次多项式必为 n 个一次式之积，当然是可约的．

定义 1　域 E 称为是代数封闭的，如果 E 没有真的代数扩张．此时亦说 E 是个**代数封闭域**．

所说 E 没有真的代数扩张的意思是，如果域 K 是 E 的代数扩张，那么必有 $K=E$．

命题 1　域 E 是代数封闭域的充分必要条件是 $E[x]$中的不

可约多项式均为 1 次的.

证明 如果 E 是代数封闭的,$p(x)$是 $E[x]$的一个不可约多项式,那么,据 §1 命题 1,我们可做 E 的一个代数扩张 $E(\lambda)$, λ 在 E 上的极小多项式为 $p(x)$.若 $\deg p(x)\neq 1$,则 $\lambda\notin E$, $E(\lambda)$ 是 E 的真的代数扩张,矛盾.故 $p(x)$的次数为 1.

反之,如果 E 上不可约多项式必为 1 次的,而 K 是 E 的代数扩张,那么,任取 $a\in K$, a 是 E 上代数元,a 满足 E 上一不可约多项式

$$e_1x-e_2,\quad e_1,e_2\in E,\ e_1\neq 0;$$

即 $e_1a=e_2$, $a=e_1^{-1}e_2\in E$.从而 $K=E$.所以,E 是代数闭域. ▌

利用"超穷集合理论"中的 Zorn 引理,可以证明,每个域一定有一个扩张域,该扩域本身是代数封闭的.

这个事实是很有用的,是很多代数学分枝中都要经常使用的.而 Zorn 引理更不仅限于在代数学中反复使用,它也是几乎所有抽象数学学科处理无穷集合或过程的必用工具.

有兴趣的读者可以在一些并不高深的"近世代数"教程中找到有关内容.本书不做详细介绍.本节就一种简单情况做些讨论,使读者能大致知道解决这一问题的几个步骤.

定义 2 设 F 是个域,$f(x)$是 F 上的一个 n 次多项式.F 的扩张域E 称为是$f(x)$的**分裂域**,如果

(1) $f(x)$作为 E 上的多项式(因为 $F\subseteq E$)可以分解为一次多项式之积

$$f(x)=a(x-a_1)\cdots(x-a_n),\quad a_i\in E;$$

(2) 对于任意扩张域 G, $F\subseteq G\subseteq E$,只要 $G\neq E$,则 $f(x)$不能有如上的一次式乘积分解形式.

这个定义中,F 上的多项式有时看作是 E 上多项式在 $E[x]$ 中分解,有时讨论它做为 G 上多项式在$G[x]$中分解.多项式分解在不同域上可达到不同程度,我们必须随时注意是在哪个域上讨论问题.

例 1 实数域 **R** 上的多项式 x^2+1 是 2 次的,复数域 **C** 是 x^2+1的一个分裂域,因为

(1) x^2+1 视为复数域 **C** 上多项式,有

$$x^2+1=(x+\mathrm{i})(x-\mathrm{i}),\quad 1,\mathrm{i},-\mathrm{i}\in\mathbf{C}.$$

(2) 若还有 **R** 的扩域 G, $\mathbf{R}\subseteq G\subseteq\mathbf{C}$,使

$$x^2+1=(x-g)(x-h),\quad g,h\in G,$$

则必有 $g+h=0, gh=1$,即 $gg=-1$,而

$$g\in G\subseteq\mathbf{C},$$

故必有 $g=\pm\mathrm{i}$. 我们知道,$\mathrm{i}\in G$,则 $\mathbf{C}\subseteq G$,故知 $\mathbf{C}=G$.

C 为 x^2+1 的一个分裂域.

例题 1 有理数域 **Q** 上的多项式 x^2+1 亦有分裂域,但复数域 **C** 不是有理数域 **Q** 上 2 次多项式 x^2+1 的一个分裂域.

证明 看复数域 **C** 的子域 $\mathbf{Q}(\mathrm{i})$. x^2+1 作为 $\mathbf{Q}(\mathrm{i})$上的多项式有

$$x^2+1=(x+\mathrm{i})(x-\mathrm{i}),\quad 1,\mathrm{i},-\mathrm{i}\in\mathbf{Q}(\mathrm{i}).$$

而 $\mathbf{Q}(\mathrm{i})$是 **C** 的真子域,故复数域 **C** 不是有理数域 **Q** 上多项式 x^2+1 的分裂域.

进一步,如果有 $\mathbf{Q}(\mathrm{i})$的子域 $G\supseteq\mathbf{Q}$,且在 G 上 x^2+1 可分解为一次式之积,相伴不论,可设

$$x^2+1=(x-g)(x-h),\quad g,h\in G.$$

由于 $G\subseteq\mathbf{Q}(\mathrm{i})$,此等式也是 $\mathbf{Q}(\mathrm{i})[x]$上的分解,但

$$x^2+1=(x-g)(x-h)=(x-\mathrm{i})(x+\mathrm{i}),\quad g,h,\mathrm{i}\in\mathbf{Q}(\mathrm{i})$$

成立,再援引分解唯一性,立刻可得到

$$g=\pm\mathrm{i},\quad h=\pm\mathrm{i}.$$

进而,由 $g=\pm\mathrm{i}$ 可推出 $\mathbf{Q}(\mathrm{i})\subseteq G$.

$\mathbf{Q}(\mathrm{i})$是有理数域 **Q** 上多项式 x^2+1 的一个分解域. ▌

命题 2 设 F 是个域,$f(x)$是 F 上 n 次多项式,E 是 F 的一个扩张域. 如果 $f(x)$作为 E 上多项式可分解为一次式之积

$$f(x)=a(x-a_1)\cdots(x-a_n),\quad a_i\in E,$$

那么，$F(a_1,\cdots,a_n)$就是 F 上多项式$f(x)$的一个分裂域.

证明 由于

$$f(x)=a(x-a_1)\cdots(x-a_n),\quad a_i\in E$$

且 $a_1,\cdots,a_n\in F(a_1,\cdots,a_n)$，上分解式乃是 F 的扩张域 $F(a_1,\cdots,a_n)$上的分解，即

$$f(x)=a(x-a_1)\cdots(x-a_n),\quad a_i\in F(a_1,\cdots,a_n).$$

进一步，如果有 $F(a_1,\cdots,a_n)$的子域 $G\supseteq F$，F 上多项式$f(x)$作为 G 上多项式分解为

$$f(x)=a(x-b_1)\cdots(x-b_n),\quad b_i\in G,$$

那么，它同时又可以看成是 $F(a_1,\cdots,a_n)$上的等式，故，在 $F(a_1,\cdots,a_n)$上，有

$$a(x-b_1)\cdots(x-b_n)=a(x-a_1)\cdots(x-a_n),$$
$$a_i,b_j\in F(a_1,\cdots,a_n).$$

据分解唯一性，调整顺序，必有

$$b_1=a_1,\quad b_2=a_2,\quad \cdots,\quad b_n=a_n.$$

这说明，$a_1,\cdots,a_n\in G$，$F(a_1,\cdots,a_n)\subseteq G$，导致

$$G=F(a_1,a_2,\cdots,a_n).$$

域 $F(a_1,\cdots,a_n)$是 F 上多项式$f(x)$的一个分裂域. ▌

定理 1 对任意域 F 上的任意多项式$f(x)$，$\deg f(x)\geqslant 1$，均有 F 的扩张域K，K 是F 上多项式$f(x)$的一个分裂域.

证明 对多项式 $f(x)$的次数用数学归纳法. 当 $\deg f(x)=1$ 时，取 $K=F$ 即可，因为 $f(x)$在 F 上就已经是一次式了.

现假定任意域上任意次数小于 n 的多项式均有分裂域，而 $f(x)$是域 F 上的n 次多项式.

设 $p(x)\in F[x]$是 $f(x)$的一次不可约的因式. 据 §1 定理 1，必有 F 的单纯代数扩张$F(\lambda)$，

$$F(\lambda)\cong F[x]/(p(x)),$$

λ 满足F 上多项式$p(x)$. 从而在 $F(\lambda)$上，

$$p(x)=(x-\lambda)q(x),\quad q(x)\in F(\lambda)[x].$$

从而,在 $F(\lambda)$上,有

$$f(x)=(x-\lambda)q(x)g(x),\quad q(x),g(x)\in F(\lambda)[x].$$

据归纳法假定,对于域 $F(\lambda)$上的 $n-1$ 次多项式 $q(x)g(x)$,必有 $F(\lambda)$的扩张域 E, E 为$F(\lambda)$上多项式 $q(x)g(x)$的一个分裂域,即 $q(x)g(x)$在 $E[x]$中可写成一次式乘积,

$$g(x)q(x)=a(x-a_2)\cdots(x-a_n),\quad a_i\in E,$$

从而有

$$f(x)=(x-\lambda)g(x)q(x)=a(x-\lambda)(x-a_2)\cdots(x-a_n),$$

其中 a 是$f(x)$的首系数,$\lambda,a_2,\cdots,a_n\in E$.

由于 $f(x)$在 E 上分解成一次式乘积,据命题 1,$F(\lambda,a_2,\cdots,a_n)$就是 F 上多项式$f(x)$的一个分裂域. ▌

下面是本节定理 1 证明中各域的关系图式

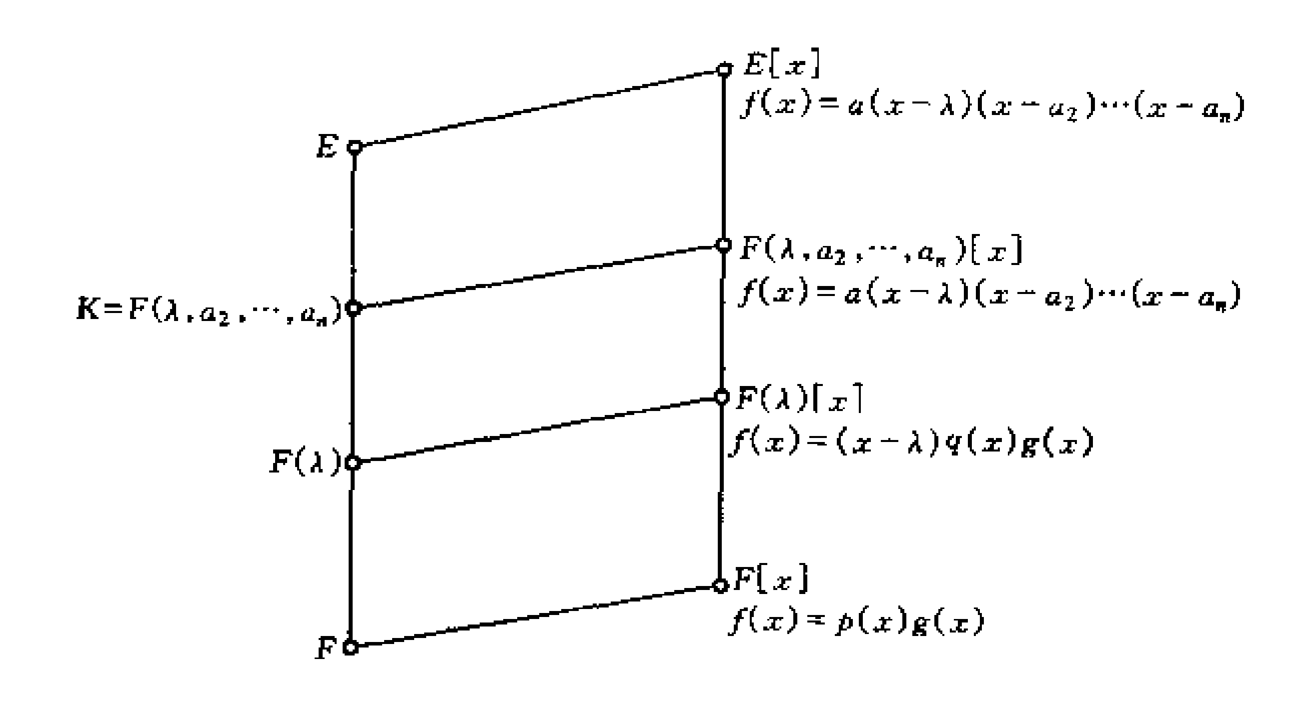


图 7-3

定理 1 告诉我们,任给一个域 F,任取其上一多项式 $f(x)$,都可以找到 F 的一个扩张域K,$f(x)$作为 K 上的多项式"彻底分

解"成一次式之积.

当然,将 F 作扩张得 $f(x)$ 的分裂域 K,也可能使其他某些的 F 上的多项式能"搭车"被彻底分解成一次式之积.

例如,取有理数域 $\mathbf{Q}$ 上二次多项式 x^2-2,得 x^2-2 的一个分裂域 $\mathbf{Q}(\sqrt{2})$. 此次扩张可使 $\mathbf{Q}$ 上很多多项式在 $\mathbf{Q}(\sqrt{2})$ 上被彻底分解,如

$$x^2-8=(x+2\sqrt{2})(x-2\sqrt{2}),$$

$$9x^2-2=(3x-\sqrt{2})(3x+\sqrt{2}),$$

$$x^4-4x^2+4=(x-\sqrt{2})(x-\sqrt{2})(x+\sqrt{2})(x+\sqrt{2}).$$

甚至,也有可能对某个多项式做了分裂域后,原域上的所有多项式"碰巧"都可以在此多项式的分裂域上被彻底分解.

例如,做实数域 $\mathbf{R}$ 上多项式 x^2+1 的分裂域 $\mathbf{C}=\mathbf{R}(\mathrm{i})$,实数域 $\mathbf{R}$ 上的任何多项式则可在复数域上被彻底分解. 也就是说,$\mathbf{R}$ 上多项式 x^2+1 的分裂域 $\mathbf{C}$ 已经是代数封闭域了.

要想在任意一个域 F 上找一个多项式 $f(x)$,使得 $f(x)$ 的一个分裂域是个代数封闭域,一般来说,是办不到的.

通常,只能像做 $\mathbf{Q}$ 上 x^2-2 的分裂域 $\mathbf{Q}(\sqrt{2})$ 那样,有些多项式能"搭车"被彻底分解,有些仍不能分成一次式之积. 如 $\mathbf{Q}$ 上 x^2-3,在 $\mathbf{Q}(\sqrt{2})$ 上仍然是不可约的.

于是,有人会想,可否再做一多项式的分裂域,又可搭车解决另一部分多项式被彻底分解问题…….

因为我们不管用多大精力如此做下去也只能完成有限步,这就需要考虑用归纳法了.

用超穷归纳法可以证明,每个域都有一个代数封闭的扩张域.

作为本书的最后一个例题,我们使用大家熟悉的数学归纳法处理小范围问题,读者知道大概意思就行了.

例题 2* 设 F 是个域. 如果有域 F 到自然数集 $\mathbf{N}$ 的单射 φ 存在,那么 F 必有一代数扩张域 E, E 是代数封闭的.

证明 只要有 F 到 $\mathbf{N}$ 的单的映射 φ 存在，我们必可建立一个 $F[x]$到 $\mathbf{N}$ 的单射 θ.

先将所有的素数按大小用自然数标上号，

$$p_0=2,\ p_1=3,\ p_2=5,\ p_3=7,\ p_4=11,\ \cdots.$$

任取 F 上多项式

$$f(x)=a_0+a_1x+\cdots+a_nx^n,\quad a_i\in F.$$

那么 $\varphi(a_i)$即为 $\mathbf{N}$ 中数. 而数

$$p_0^{\varphi(a_0)}p_1^{\varphi(a_1)}\cdots p_n^{\varphi(a_n)}\in\mathbf{N}$$

是由 $\varphi(a_0),\varphi(a_1),\cdots$唯一确定的，从而由 $f(x)$完全确定.

$$\theta: a_0+a_1x+\cdots+a_nx^n\to p_0^{\varphi(a_0)}p_1^{\varphi(a_1)}\cdots p_n^{\varphi(a_n)}$$

就是 $F[x]$到 $\mathbf{N}$ 的一个映射.

然后可以证明 θ 是个单射. 设

$$f(x)=a_0+a_1x+\cdots+a_nx^n\in F[x],$$

$$g(x)=b_0+b_1x+\cdots+b_mx^m\in F[x],$$

使得 $\theta(f)=\theta(g)$，即

$$p_0^{\varphi(a_0)}p_1^{\varphi(a_1)}\cdots p_n^{\varphi(a_n)}=p_0^{\varphi(b_0)}p_1^{\varphi(b_1)}\cdots p_m^{\varphi(b_m)}.$$

那么，由整数分解唯一定理，必有 $m=n$ 且

$$\varphi(a_0)=\varphi(b_0),\ \cdots,\ \varphi(a_n)=\varphi(b_n).$$

同时因为 φ 是个单射，故必有

$$a_0=b_0,\ a_1=b_1,\ \cdots,\ a_n=b_n,$$

也就是 $f(x)=g(x)$，θ 是个单射.

现在，做 F 的一系列扩张域，每个自然数 n 对应一个扩张域.

F 的第一个扩张域就是 F 自己.

F 的第二个扩张域决定于数 2 是不是某个 $f(x)$在 θ 之下对应过来，如果有 $f(x)\in F[x]$，

$$\theta(f)=2,$$

那么，F 的第二扩张域就取此 $f(x)$的一个分裂域. 如果任何 $f(x)$

都不对应 2,F 的第二扩张域仍取 F 本身;

F 的第三扩张域取决于数 3 是否为某多项式的 θ 之下的像.若 $\theta(g)=3$,第三扩张等于 $g(x)$在第二扩域上做的分裂域,若 3 不为任何 $g(x)$的像,取第三扩张域等于第二扩张域…….

这个定义方法可以归纳给出.用 $\Phi(n)$代表 F 的第 n 个扩张域.

当 $n=1$ 时,$\Phi(1)=F$.

当 $n>1$ 时,规定

$$\Phi(n+1)=\begin{cases}\Phi(n), & \text{如果 } n \text{ 不是任何多项式在}\theta\text{ 下的像},\\ \text{为 } f(x)\text{在 } \Phi(n)\text{上分裂域}, & \text{如果 } \theta(f)=n.\end{cases}$$

这样,我们得到的就不只是有限个扩张域,而是得到了无穷多个,它们有关系

$$F=\Phi(1)\subseteq\Phi(2)\subseteq\cdots\subseteq\Phi(n)\subseteq\Phi(n+1)\subseteq\cdots.$$

令 E 是这些集合的并集,即

$$E=\bigcup_{n\in N}\Phi(n).$$

再想办法把 E 定义成一个域,而且诸 $\Phi(n)$要是它的子域.

对任意 $a,b\in E$.因为 E 是个并集,从而必有 $m,n\in N$ 使

$$a\in\Phi(n),\quad b\in\Phi(m).$$

但诸 $\Phi(n)$有包含关系,设 $m\leqslant n$,则 $a,b\in\Phi(n)$.而 $\Phi(n)$是个域.我们规定 a,b 在E 中之和以及之积的元素就是它们在 $\Phi(n)$中的之和元素与之积元素.

由于诸 $\Phi(i)$中,号大者为号小者扩张域,其运算是一致的,上述 E 中和与积的运算不受算号影响;也就是说,如果取 $l\geqslant m,n$,在任何 $\Phi(l)$中,所得的和元素与积元素均不变化.

很容易验证,E 在这两运算之下构成域,每个 $\Phi(n)$均可视为 E 的一个子域.

进一步,任意 $a\in E$,必有 $m\in N$,使 $a\in\Phi(m)$,而 $\Phi(m)$是 F 的第 m 次扩张,每次扩张(或不动或做一多项式的分裂域)都是

一个代数扩张. 由§3知 $\Phi(m)$ 为 F 的代数扩张, a 为 F 上的代数元, 从而 E 是 F 的一个代数扩张.

最后, 可以证明 E 是个代数闭域. 设 K 是 E 的一个真的代数扩张, $a\in K$, $a\notin E$. 那么, K 必为 F 的代数扩张, a 为 F 上的代数元. 所以, a 满足 F 上的一个不可约多项式 $p(x)$. 设

$$\theta(p(x))=k,\quad k\in N,$$

于是 F 的第 $k+1$ 次扩张 $\Phi(k+1)$ 是 $\Phi(k)$ 上多项式 $p(x)$ 的分裂域. 换言之, 在 $\Phi(k+1)$ 上应有

$$p(x)=a_0(x-a)(x-a_1)\cdots(x-a_t),\quad a_i\in\Phi(k+1),$$

同时, $a\in\Phi(k+1)$, 矛盾.

证明得以全部完成. ▍

习　题　四

1. 看有理数域 $\mathbf{Q}$ 上的多项式 $f(x)=x^3-3x+1$, 证明: 若 $\alpha\in\mathbf{C}$ 是 $f(x)$ 的 1 个根, 则 α^2-2 和 $2-\alpha-\alpha^2$ 必为 $f(x)$ 另外 2 个根. 从而 $f(x)$ 的分裂域就是 $\mathbf{Q}(\alpha)$.

2*. 证明: 任何有限域都不是代数封闭的.

3. 证明: §3 例题 1 中的域 $G=\{a\in\mathbf{C}\mid a$ 是 $\mathbf{Q}$ 上的代数元$\}$ 是个代数封闭域.

小　　结

本章讨论一个给定域 F 的各种扩张域, 这些扩张的关系可画成如下图 7-4.

矩形 $ABDC$ 代表 F 的所有扩张域的集合, 矩形 $AEFC$ 代表域 F 之所有无限扩张域的集合, 矩形 $EBDF$ 代表域 F 的所有有限扩张域的集合, 而矩形 $GBDH$ 代表 F 的所有代数扩张域的集合, 三角形 LFD 代表 F 的所有单纯代数扩张域的集合, 三角形 KHC 代表 F 的所有单纯超越扩张的集合, 两个三角形的并就是所有单

纯扩张的集合.实际上就是

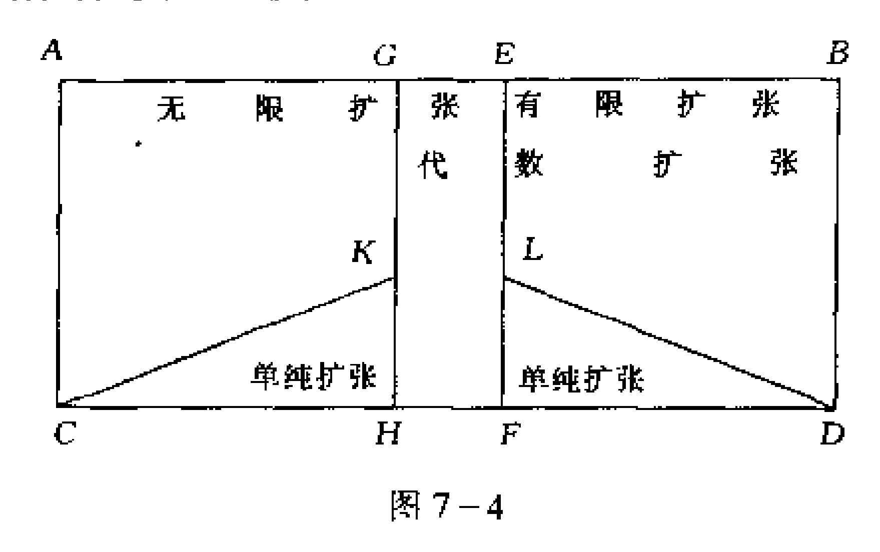


图 7－4

{单纯代数扩张}⊂{有限扩张}⊂{代数扩张},

{超越单纯扩张}⊂{无限扩张},

{单纯扩张}＝{单纯代数扩张}∪{单纯超越扩张}.

读者在复习本章时一定要搞清上述关系,心中应当有一批例子来说明哪些扩张是不等价的概念,哪些是大概念、哪些是小概念.

单纯扩张,即把一个单个元素添加到 F 上生成的域,是研究所有各种扩张的基础.因为 F 的任何扩张域都是 F 又添上 1 个、多个或无穷多个元素生成的.

域 F 上添加一个元素 a 生成的扩域 $F(a)$ 的结构决定于 $1,a,a^2,\cdots,a^m,\cdots$ 在 F 上是否线性相关以及相关时的系数(也就是 a 满足 F 上某个多项式).所以 §1 之命题 1 的结论和证明方法都比较重要.

对于域 F 的有限扩张 K,因为有了定量的刻画工具 $[K:F]$,研究 F 与 K 中间的域 E,

$$F\subseteq E\subseteq K,$$

则有 $[E:F][K:E]=[K:F]$,这就是 §2 的定理 1,要求读者能够灵活运用这一工具.

域 F 上的代数元 a 与 F 上的一个不可约多项式密切相联

(a 的极小多项式),而多项式的可约性与具体分解涉及到第六章的较深入的内容,如果读者在判定多项式的根与可约性等方面遇到困难,应当及时复习第六章的有关内容.

复 习 题

1. 在 $\mathbf{Q}(\sqrt[3]{2})$求 $1+\sqrt[3]{2}+\sqrt[3]{4}$的逆.

2. 问下列配好的 6 对域中,相应的 2 个域是否相等,并说明理由.

(a) $\mathbf{Q}(\sqrt{5})$和 $\mathbf{Q}(1+\sqrt{5})$;

(b) $\mathbf{Q}(1+\sqrt{3})$和 $\mathbf{Q}(\sqrt[4]{3})$;

(c) $\mathbf{Q}(\sqrt{2})$和 $\mathbf{Q}(\sqrt{2}-2)$;

(d) $\mathbf{Q}(\sqrt[3]{2})$和 $\mathbf{Q}(\sqrt[3]{4})$;

(e) $\mathbf{Q}(\sqrt{5})$和 $\mathbf{Q}(\sqrt{7})$;

(f) $\mathbf{Q}(\sqrt[4]{2})$和 $\mathbf{Q}(\sqrt[4]{8})$.

3. 设 K 是域 F 的一个扩张域. 证明:K 是 F 的有限扩张的充分必要条件是有 K 上代数元 $a_1,\cdots,a_n$ 使得 $K=F(a_1,a_2,\cdots,a_n)$.

4. 在 $\mathbf{C}[x]$中利用公式

$$(x+s+t)\mid(x^3-3stx+s^3+t^3)$$

找出$\sqrt[3]{2}+\sqrt[3]{4}$在有理数域 $\mathbf{Q}$ 上的极小多项式.

5. 如果 a 是域 F 上的代数元,a 在 F 上的极小多项式是 $g(x)$, $g(x)$ 的次数是个奇数,证明:$F(a)=F(a^2)$.

6*. 设 K 是域 F 的扩张域,$S\subseteq K$. 如果 $a\in K$ 是 $F(S)$上的代数元,证明:一定有 S 的有限子集 T 使得 a 是 $F(T)$上的代数元.

7*. 验证:域 $\mathbf{Q}(\sqrt{3},\mathrm{i})$是有理数域 $\mathbf{Q}$ 上多项式 $f(x)=(x^2-2x-2)(x^2+1)$的分裂域.

习题解答与提示

第一章　集合、映射和关系

习　题　一

1. 用描述方式写出集合.

(a) $\{x \in \mathbf{I} \mid$ 有正整数 n 使得 $x = -2n+1\}$;

(b) $\{x$ 是日期 $\mid x$ 是春季某月的第一天$\}$;

(c) $\left\{x \in \mathbf{R} \mid x > 0 \text{且 } x = \dfrac{n-1}{n},\ n \text{ 为正整数}\right\}$;

(d) $\{x \in \mathbf{I} \mid x$ 是在数 3.14159 中出现的数字$\}$.

2. 列举元素.

(a) $\{-6, -5, -4, \cdots\}$;

(b) $\{2,3,5,7,11,13,17,19,23,29,31,37,41,43,47\}$;

(c) $\{(1,2),(-1,-2)\}$;

(d) $\left\{\dfrac{1}{2},\dfrac{1}{3},\dfrac{2}{3},\dfrac{1}{4},\dfrac{3}{4},\cdots\right\}$;

(e) {1 月,2 月,3 月,5 月,7 月,8 月,10 月,12 月}.

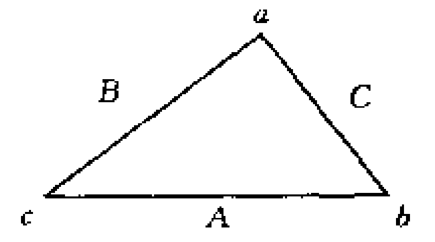
(f) $\{-1\}$. 这是因为,首先可断言 $m=0$. 若不然,由

$$n^2-1=2m,\quad n+1=4m$$

可导致 $n-1=(2m)/(4m)=\dfrac{1}{2}$, n 不为整数. 故

$$n+1=0,\quad n=-1.$$

3. 记三角形如图，则



$A \cap B = \{c\}$,

$A \cap B \cap C = \varnothing$,

$A \cup B \cup C = \{$三角形 3 个边上所有的点$\}$.

6. $\bigcap_{n \in \mathbf{I}} I_{(n)} = \{0\}$, $\bigcup_{n \in \mathbf{I}} I_{(n)} = \mathbf{I}$.

7. $B \cup C - B \cap C = 2 \cup 4 \cup 3 \cup 6$,

$A \cap (B \cup C - B \cap C) = 4 \cup 6$,

$(A \cap B) \cup (A \cap C) = 4 \cup 7 \cup 6$,

$(A \cap B) \cup (A \cap C) - A \cap B \cap C = 4 \cup 6$.

习　题　二

1. 给出笛卡尔积 $A \times B$.

(a) $\{(1,2),(1,3),(1,1),(2,1),(2,2),(2,3)\}$;

(b) $\{(1,1),(1,2),(1,3),(1,4),(1,5)(1,6)\}$;

(c) $\{(x,y) \mid x,y \in \mathbf{R},\ x \leqslant 0,\ y \geqslant 1\}$;

(d) $\{(x,y) \in \mathbf{R} \times \mathbf{I} \mid x \leqslant 0\}$;

(e) $\{(1,1),(2,1),(3,1),(4,1),(5,1),(6,1)\}$;

(f) $\{(x,y) \in \mathbf{I} \times \mathbf{I} \mid y \leqslant 0\}$;

(g) $\{(1,1),(1,2),(2,1),(2,2)\}$;

(h) $\{((1,1),1),((1,2),1),((2,1),1),((2,2),1),((1,1),2),((1,2),2),((2,1),2),((2,2),2)\}$;

(i) $\{(1,(1,1)),(1,(1,2)),(1,(2,1)),(1,(2,2)),(2,(1,1)),(2,(1,2)),(2,(2,1)),(2,(2,2))\}$.

2. 解释关系.

(a) $\{(a,b) \in A \times B \mid a,b$ 均为偶数$\}$;

(b) $\{(a,b) \in A \times B \mid b$ 为奇数$\}$;

(c) $\{(a,b) \in A \times B \mid b - a = 10\}$.

3. 给出关系子集.

(a) $\{(2,4),(2,6),(2,8),(2,10),(2,12),(3,6),(3,9),(3,12),(4,8),(4,12),(5,10),(6,12)\}$;

(b) $\{(10,11),(11,10),(9,12),(12,9)\}$;

(c) $\{(2,5),(3,7),(4,9),(5,11)\}$;

4. $\{(3,1),(-1,1),(2,2)\}$.

习 题 三

1. 列举元素.

(a) $R=\{(1,3),(1,5),(1,7),(1,9),(3,5),(3,7),(3,9),(5,7),(5,9),(7,9)\}$;

(b) $R=\{(2,3),(3,2),(2,5),(5,2),(3,4),(4,3),(3,5),(5,3),(4,5),(5,4),(5,6),(6,5)\}$;

(c) $R=\{(\varnothing,\varnothing),(\varnothing,\{x\}),(\varnothing,\{y\}),(\varnothing,\{x,y\}),(\{x\},\{x\}),(\{x\},\{x,y\}),(\{y\},\{y\}),(\{y\},\{x,y\}),(\{x,y\},\{x,y\})\}$.

2. 找漏洞.

前面说,"若"aRb,"则"bRa,这不能保证"一定"有 b,从而不能作为后面证明的依据.也就是说,可能对某个元素 a 来说,没有任何元素 b 使得 aRb,所以,以下的证明就不能成立了.

4. 对任意 $a\in A$,由于 R 和 S 确定 A 上的等价关系,故 $(a,a)\in R$ 且 $(a,a)\in S$.从而 $(a,a)\in S\cap R$.

若 $(a,b)\in S\cap R$,即 $(a,b)\in R$ 且 $(a,b)\in S$,而 R 和 S 都是 A 上等价关系,从面 $(b,a)\in S$ 且 $(b,a)\in R$,进面 $(b,a)\in S\cap R$.

若 $(a,b)\in S\cap R$, $(b,c)\in S\cap R$,即

$$(a,b)\in S,\quad (b,c)\in S,$$
$$(a,b)\in R,\quad (b,c)\in R,$$

由于 S 和 R 都满足传递性,故 $(a,c)\in R$ 而且 $(a,c)\in S$,从而

$$(a,c)\in S\cap R.$$

5. 对任意 $a\in A$，由于诸 R_n 均有反身性，即 $(a,a)\in R_n$，$n=1,2,\cdots$. 从而 $(a,a)\in\bigcup_{n\in\mathbf{N}}R_n=R$.

若 $(a,b)\in R$，而 R 是诸 R_n 的并集，故必有 $i\in\mathbf{N}$ 使得 $(a,b)\in R_i$. 由于 R_i 有对称性，故 $(b,a)\in R_i$，从而 $(b,a)\in R=\bigcup_{n\in\mathbf{N}}R_n$.

若 $(a,b)\in R$，$(b,c)\in R$，则必有 $j,k\in\mathbf{N}$ 使得 $(a,b)\in R_j$，$(b,c)\in R_k$. 我们选一个自然数 l 使得 $j\leqslant l$，$k\leqslant l$，由于

$$R_j\subseteq R_{j+1}\subseteq\cdots,\quad R_k\subseteq R_{k+1}\subseteq\cdots$$

必有 $(a,b)\in R_l$，$(b,c)\in R_l$. 而 R_l 有传递性，故 $(a,c)\in R_l$，$(a,c)\in R$.

6. 设 $A=\{x,y\}$. 那么

$$A\times A=\{(x,x),(x,y),(y,x),(y,y)\}.$$

(a) $A\times A$ 的每个子集都确定 A 上一个关系. 由于 $A\times A$ 有 16 个子集，故 A 上有 16 个不同的关系.

(e) $A\times A$ 的满足反身性的子集也就是 $A\times A$ 的含有 (x,x) 和 (y,y) 的子集，它们是

$$\{(x,x),(y,y)\},$$
$$\{(x,x),(y,y),(x,y)\},$$
$$\{(x,x),(y,y),(y,x)\},$$
$$\{(x,x),(y,y),(x,y),(y,x)\},$$

共 4 个.

(d) $A\times A$ 的具有传递性的子集是

$\varnothing,\{(x,x)\},\{(y,y)\},\{(x,y)\},\{(y,x)\}$;

$\{(x,x),(x,y)\},\{(x,y),(y,y)\},\{(y,x),(x,x)\}$;

$\{(y,x),(y,y)\},\{(x,x),(y,y)\}$;

$\{(x,x),(x,y),(y,y)\},\{(x,x),(y,x),(y,y)\}$;

$\{(x,y),(y,x),(x,x),(y,y)\}$.

共计 13 个.

(c) $A\times A$ 的具有对称性的子集是

$\varnothing,\{(x,x)\},\{(y,y)\},\{(x,y),(y,x)\},\{(x,x),(y,y)\};$

$\{(x,y),(y,x),(x,x)\},\{(x,y),(y,x),(x,x)\};$

$\{(x,x),(x,y),(y,x),(y,y)\}.$

共计 8 个.

(b) 属于上述(c),(d),(e)中共有的子集是

$\{(x,x),(y,y)\},\quad \{(x,x),(y,y),(x,y),(y,x)\},$

从而 A 上只有两个等价关系.

(f) 二元集 A 只有两种分类方法,一是整个集合 $A=\{x,y\}$ 为一个等价类;一是分成两个等价类,$\{x\}$为一等价类,$\{y\}$为另一个等价类.

习 题 四

1. $(f\circ f)(x)=x^4$, $(g\circ g)(x)=x+2$, $((g\circ f)\circ g)(x)=(x+1)^2+1$, $((f\circ g)\circ f)(x)=(x^2+1)^2$.

3. 对任意 $x\in A$,由 $(h\circ f)(x)=(h\circ g)(x)$ 即 $h(f(x))=h(g(x))$和 h 为单射知$f(x)=g(x)$.

4. 对任意 $y\in B$,由于 h 是满的,必有 $x\in A$ 使 $y=h(x)$. 于是,由$(f\circ h)(x)=(g\circ h)(x)$, $f(h(x))=g(h(x))$, $f(y)=g(y)$推出 $f=g$.

5. 由于 f 和 g 是单射知 $g\circ f$ 为单射,由 f 和 g 是满的又知 $g\circ f$是满的.

又,$f^{-1}\circ g^{-1}:C\to A$,且$(f^{-1}\circ g^{-1})\circ(g\circ f)=f^{-1}\circ(i_B\circ f)=f^{-1}\circ f=i_A$,同理$(g\circ f)\circ(f^{-1}\circ g^{-1})=i_C$. 再由逆映射的唯一性,得$(g\circ f)^{-1}=f^{-1}\circ g^{-1}$.

6. $a\neq0$, $a\neq0$.

8*. 若 $z\in \mathrm{Img}(g\circ f)$,则有 $x\in A$,使 $z=(g\circ f)(x)$,即 $z=g(f(x))$. 由于 $f(x)\in \mathrm{Img}(f)$,故

$$g(f(x))\in g(\mathrm{Img}(f)).$$

反之,如果 $z\in g(\mathrm{Img}(f))$,则有 $y\in \mathrm{Img}(f)$使 $z=g(y)$. 而

$y \in \mathrm{Img}(f)$则必有 $x \in A$ 使 $y = f(x)$. 故

$$z = g(y) = g(f(x)) = (g \circ f)(x) \in \mathrm{Img}(g \circ f).$$

习　题　五

1. 求反序数.

(a) $n(n-1)/2$;　(b) $n(n-1)/2$.

2. 求置换复合.

$$P_2 \circ P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad P_5 \circ P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$P_3 \circ P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad P_4 \circ P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

3. 求逆置换.

$$\begin{pmatrix} 2 & 4 & 3 & 6 & 1 & 5 \\ 1 & 5 & 4 & 3 & 2 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 5 & 6 & 3 \end{pmatrix}.$$

4*. 用 P^i 代表 i 个置换 P 依次复合

$$P^i = ((P \circ P) \circ \cdots) \circ P, \quad i < n,$$

则 $P^i(n) = i \neq n$. 故 $P^i \neq I$, I 是$\{1,2,\cdots,n\}$上恒等映射. P 是双射,对所给 n 个置换用消去办法可说明它们两两不同.

习　题　六

1. 验证结合律与交换律.

(b)和(d)满足结合律;(a),(c),(d)满足交换律.

2. 完成运算表.

$\cdot$	x	y	z	w
x	x	z	w	y
y	z	y	x	w
z	w	x	y	y
w	y	w	y	x

3. 设

$$r+s=qn+k,\quad 0\leqslant k<n,$$
$$k\times t=pn+l,\quad 0\leqslant l<n,$$
$$r\times t=xn+i,\quad 0\leqslant i<n,$$
$$s\times t=yn+j,\quad 0\leqslant j<n,$$

即 $r^*+s^*=k^*$, $k^*\times t^*=l^*$, $r^*\times t^*=i^*$, $s^*\times t^*=j^*$,那么,

$$i+j=zn+h,\quad 0\leqslant h<n$$

就有 $i^*+j^*=h^*$. 于是,由

$$(r+s)\times t=(r\times t)+(s\times t)$$

得

$$(qn+k)\times t=(x+y)n+i+j,$$
$$qnt+pn+l=(x+y+z)n+h.$$

由于 $0\leqslant l<n$, $0\leqslant h<n$,故 $l=h$, $l^*=h^*$. 也就是

$$(r^*+s^*)\times t^*=i^*+j^*=r^*\times t^*+s^*\times t^*.$$

5. 从运算表上可以看出

$$好\odot坏=好=坏\odot好,$$

故该运算满足交换律.

任取 $x,y,z\in A=\{好,坏\}$. 若 $x=好$,则

$$x\odot y=好,\ (x\odot y)\odot z=好,\ x\odot(y\odot z)=好.$$

从而 $x\odot(y\odot z)=(x\odot y)\odot z$. 同理,当 y 为好时,不管 x,z 为好为坏,均为

$$(x\odot y)\odot z=x\odot(y\odot z).$$

当 z 为好时,亦可照此办理.

若 x,y,z 均为坏时,$x\odot y$ 和 $y\odot z$ 亦坏,从而恒有

$$(x\odot y)\odot z=x\odot(y\odot z)=坏.$$

元素"坏"是 A 的恒等元,因为

$$好\odot坏=坏\odot好=好,\quad 坏\odot坏=坏.$$

6. 由于

$$(1\odot 1)\odot 1=(2+1)\odot 1=2\times 3+1=7,$$
$$1\odot(1\odot 1)=2+3^2=11.$$
故该运算不满足结合律.

又由于

$$1\odot 0=2,\quad 0\odot 1=1,$$
故此运算不适合交换律.

如果 $e\in\mathbf{I}$ 是恒等元,则对任意 $m\in\mathbf{I}$ 必有

$$e\odot n=2e+n^2=n,$$
即对任意 $n\in\mathbf{I}$, $2e=n-n^2$,这是不可能的,因为

$$1-1^2=0,\quad 2-2^2=-2.$$

复 习 题

3. 对任意 $x\in B-\bigcup\limits_i A_i$,由于 $x\in B$ 但

$$x\notin\bigcup_{i\in\mathbf{I}}A_i$$
知 x 不属于任何一个 A_i, $i\in\mathbf{I}$. 从而,对每个 $i\in\mathbf{I}$ 都有 $x\in B$, $x\notin A_i$,也就是 $x\in B-A_i$. 进而 $x\in\bigcap\limits_{i\in\mathbf{I}}(B-A_i)$.

反过来,若 $x\in\bigcap\limits_{i\in\mathbf{I}}(B-A_i)$,那么,对每个 $i\in\mathbf{I}$ 都有 $x\in B-A_i$,即 $x\in B$,x 不属于每个 A_i. 从而 $x\notin\bigcup\limits_{i\in\mathbf{I}}A_i$,故

$$x\in B-\bigcup_{i\in\mathbf{I}}A_i.$$

4. (a) 是个映射关系,因为每个 $m\in\mathbf{I}$ 都出现在(a)中元素的第一个位置上,而且只出现一次;

(b) 不是映射关系,有的整数不出现在(b)的元素第一位置上. 例如,(b)中没有形如

$$(1,*)$$
的元素,即 $1\in\mathbf{I}$,但它在第二个位置上找不到对应元素;

也不是映射关系,它有元素

$$(1,1),\quad(-1,1),$$
就是说,$\mathbf{I}$ 中有元素在(c)的第一位置上出现次数多于一次;

对于集合(d),由于

$$\{(m,2m+1)\mid m\in\mathbf{I}\}=\{(m-1,2m-1)\mid m\in\mathbf{I}\},$$

任何 $m\in\mathbf{I}$ 均在(d)的元素第一个位置上出现且只出现一次,(d)是个映射关系.

5. 前半部分关于反身性、对称性和传递性的证明是显然的.因为

$$(-2)^2=(2)^2=4,\quad 0^2=0,$$
$$(-1)^2=1^2=1,\qquad 3^2=9,$$

故 R 含 6 个元素,它们是

$$(-2,4),(2,4),(-1,1),(1,1),(0,0),(3,9).$$

7. $f^{-1}(S_1)=g^{-1}(S_1)=\mathbf{I}$;

$g^{-1}(S_2)=\{1,-1\},f^{-1}(S_2)=\{1,-1,\mathrm{i},-\mathrm{i}\}$;

$g^{-1}(S_3)=\{\sqrt{m},-\sqrt{m}\mid m\in\mathbf{I},\ m\geqslant 0\}$;

$f^{-1}(S_3)=\{\sqrt{m},-\sqrt{m},\mathrm{i}\sqrt{m},-\mathrm{i}\sqrt{m}\mid m\in\mathbf{I},\ m\geqslant 0\}$;

这里的 i 代表纯虚数.

8. 令 $g(1)=1$,且对任意 $j>1$, $g(j)=j-1$,那么,g 是 $\mathbf{N}$ 到 $\mathbf{N}$ 的映射,且

$$(g\cdot f)(1)=g(f(1))=g(2)=2-1=1,$$

对任意 $j>1$,有

$$(g\cdot f)(j)=g(f(j))=g(j+1)=j,$$

从而 $g\cdot f$ 使 $\mathbf{N}$ 的每个元素都不动,$g\cdot f$ 为 $\mathbf{N}$ 上的恒等映射.

仔细分析一下,上面定义中规定 $g(1)=1$ 是可以随便改变的.因为在验证等式时根本没涉及到 $g(1)$ 为何值.于是,改变 $g(1)$ 的定义就可得到无穷多个映射满足要求.

对任意 $h:\mathbf{N}\to\mathbf{N}$,必有

$$(f\cdot h)(1)=f(h(1))=h(1)+1,$$

由于 $h(1)\in\mathbf{N}$,故 $h(1)+1\neq 1$.也就是说,$f\cdot h$ 不能使 1 保持不动,从而 $f\cdot h$ 不是恒等映射.

第二章 群与子群

习 题 一

1. 因为

$$(f\cdot g)(x)=f(g(x))=f(1/x)=1/x=g(x),$$
$$(g\cdot f)(x)=g(f(x))=g(x),$$
$$(f\cdot f)(x)=f(f(x))=f(x),$$
$$(g\cdot g)(x)=g(g(x))=g\left(\frac{1}{x}\right)=x=f(x),$$

即 $f\cdot g=g$，$g\cdot f=g$，$f\cdot f=f$，$g\cdot g=f$，所以映射的复合确实是 $\{f,g\}$ 上的一个运算.

映射复合是满足结合律的.

f 是 $\{f,g\}$ 的恒等元，f 是 f 的逆元，g 是 g 的逆元.

2. 由

$$a\cdot(b\cdot c)=a\cdot[b+c-2]=a+(b+c)-2-2,$$
$$(a\cdot b)\cdot c=(a+b-2)\cdot c=a+b-2+c-2,$$

知运算满足结合律.也容易看出运算是可交换的.

取整数集 $\mathbf{I}$ 之元素 2，对任意 $a\in\mathbf{I}$，有 $2\cdot a=a+2-2=a$.从而 2 是恒等元.

对每个 $a\in\mathbf{I}$，由于 $(4-a)\cdot a=4+a-a-2=2$，即知 $4-a$ 是 a 的逆元.

4. 任取 $f,g,h\in F$，

$$[(f\# g)\# h](x)=(f\# g)(x)+h(x)=(f(x)+g(x))+h(x),$$
$$[f\#(g\# h)](x)=f(x)+(g\# h)(x)=f(x)+(g(x)+h(x)),$$

故运算 # 满足结合律.容易验证交换律.

用 θ 代表 F 中每点均取值 0 的常数函数,则对任意 $f\in F$ 恒有

$$(f\#\theta)(x)=f(x)+\theta(x)=f(x),$$

即 $f\#\theta=f$.

任取 $f\in F$,我们用 $-f$ 代表这样的函数

$$(-f)(x)=-f(x),\quad x\in(-\infty,\infty),$$

那么,

$$[(-f)\#f](x)=(-f)(x)+f(x)=-f(x)+f(x)=\theta(x).$$

故 $(-f)\#f=\theta$, $-f$ 是 f 的逆元(亦可称为负元,因为 $\#$ 可交换).

5.

*	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

首先,由 $ab=b$ 知 a 为恒等元,故

$$aa=a,\quad ac=c,\quad ba=b,\quad bc=c.$$

其次,由于群中有消去律,上表中任意一行和任一列都不能出现两个相同的元;进而每行每列必然 a,b,c 出现而且只出现一次.从而由 bc 不能等于 b,也不能等于 a(否则可推出 b 或 c 为恒等元,与恒等元唯一性矛盾),故 $bc=a$, $cb=a$.

最后,根据上述同行同列不能出现相同元素的断言,必有

$$b\cdot b=c,\quad cc=b.$$

6. 若 G 为交换群,那么.

$$(ab)^{-1}=b^{-1}a^{-1}=a^{-1}b^{-1}.$$

反之,若对任意 $a,b\in G$ 恒有 $(ab)^{-1}=a^{-1}b^{-1}$,那么,对任意 $x,y\in G$,必有 $(y^{-1}x^{-1})^{-1}=(y^{-1})^{-1}(x^{-1})^{-1}$,也就是

$$[(xy)^{-1}]^{-1}=xy=(y^{-1})^{-1}(x^{-1})^{-1}=yx,$$

这说明 G 是个交换群.

7. 对任意 $x,y,z\in\mathbf{R}-\{1\}$,

$$\begin{aligned}
&(x\# y)\# z\\
&=(x+y-xy)\# z && (\#\text{的定义})\\
&=x+y-xy+z-(x+y-xy)z\\
&=x+y+z-xy-xz-yz-xyz && (\#\text{的定义})\\
&=x\#(y\# z),
\end{aligned}$$

这说明#满足结合律.而满足交换律是显而易见的.

对任意 $x\in\mathbf{R}$, $x\neq1$,恒有

$$x\#0=x+0-0=x.$$

故0为恒等元.又当 $x\in\mathbf{R}$, $x\neq1$,则 $x-1\neq0$,且

$$x\#(x/(x-1))=x+x/(x-1)-x^2/(x-1)=0,$$

即 x 必有逆元.所以,$(\mathbf{R}-\{1\},\#)$是交换群.

习 题 二

3. 当 $a,b,c;d,e,f$ 为偶数时,$d+a,f+c,e+af+b$ 均为偶数,故

$$\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\begin{pmatrix}1&d&e\\0&1&f\\0&0&1\end{pmatrix}=\begin{pmatrix}1&d+a&e+af+b\\0&1&f+c\\0&0&1\end{pmatrix}\in E.$$

又,当 a,b,c 为偶数时,$-a,-c,ac-b$ 为偶数,

$$\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}^{-1}=\begin{pmatrix}1&-a&ac-b\\0&1&-c\\0&0&1\end{pmatrix}\in E.$$

4. 若 $x,y\in H$,即 $x^m=e$, $y^m=e$,从而 $x^my^m=(xy)^m=e$, $xy\in H$.

若 $x\in H$, $x^m=e$,那么$(x^{-1})^m=(x^m)^{-1}=e^{-1}=e$,这说明 $x^{-1}\in H$.

6. 首先 $a\neq0$, $c\neq0$ 则 $ac\neq0$,所以Δ确实是 G 上的运算.

其次,任取(a,b),(c,d),$(e,f)\in G$,那么

$$((a,b)\Delta(c,d))\Delta(e,f)$$
$$=(ac,bc+d)\Delta(e,f) \qquad (定义)$$
$$=(ace,(bc+d)e+f) \qquad (定义)$$
$$=(ace,bce+de+f).$$

另一方面,

$$(a,b)\Delta((c,d)\Delta(e,f))$$
$$=(a,b)\Delta(ce,de+f) \qquad (定义)$$
$$=(ace,bce+de+f), \qquad (定义)$$

这说明 Δ 满足结合律.

再次,可以证明 $(1,0)$ 是 (G,Δ) 的恒等元. 因为,对任意 $(a,b)\in G$,有

$$(1,0)\Delta(a,b)=(a,0a+b)=(a,b),$$
$$(a,b)\Delta(1,0)=(a,b\cdot 1+0)=(a,b).$$

最后,通过解方程可以算出,对 $(a,b)\in G$ 有

$$\left(\frac{1}{a},-\frac{b}{a}\right)\Delta(a,b)=(1,-b+b)=(1,0),$$
$$(a,b)\Delta\left(\frac{1}{a},-\frac{b}{a}\right)=\left(1,\frac{b}{a}-\frac{b}{a}\right)=(1,0).$$

要证明 H 是 G 的子群,对任意 $(1,b),(1,d)\in H$,均有

$$(1,b)\Delta(1,d)=(1,b+d)\in H.$$

而 $(1,b)$ 在 (G,Δ) 中的逆元 $(1,-b)\in H$,故 H 是 G 的子群.

7. 将其乘法表列出则一目了然.

	I	A	B	C	$-I$	$-A$	$-B$	$-C$
I	I	A	B	C	$-I$	$-A$	$-B$	$-C$
A	A	$-I$	C	$-B$	$-A$	I	$-C$	B
B	B	$-C$	$-I$	A	$-B$	C	I	$-A$
C	C	B	$-A$	$-I$	$-C$	$-B$	A	I
$-I$	$-I$	$-A$	$-B$	$-C$	I	A	B	C
$-A$	$-A$	I	$-C$	B	A	$-I$	C	$-B$
$-B$	$-B$	C	I	$-A$	B	$-C$	$-I$	A
$-C$	$-C$	$-B$	A	I	C	B	$-A$	$-I$

习　题　三

1. 子群⟨(1 2 3 4)⟩共有 4 个元素

$$(1),(1\ 2\ 3\ 4),(1\ 3)(2\ 4),(1\ 4\ 3\ 2).$$

而子群⟨(1 2),(3 4)⟩的元素是

$$(1),(1\ 2),(3\ 4),(1\ 2)(3\ 4).$$

2. 4 阶交代群的元素是

(1),(1 2)(3 4),(1 3)(2 4),(1 4)(2 3),(1 2 3),(1 3 2),(2 3 4),(2 4 3),(1 3 4),(1 4 3),(1 2 4),(1 4 2).

3. 两个子群是

$$H=\{(1),(3\ 4)\},$$

$$K=\{(1),(1\ 2),(3\ 4),(1\ 2)(3\ 4)\}.$$

4. (1 3)(2 4 5),(1 3 4)(2 5),(1 2 3 4 5),(5 4 3 2 1).

5*. (1),(1 2),(3 4),(1 2)(3 4).

习　题　四

1. 子群有 4 个:

(a) {[0],[1],[2],[3],[4],[5],[6],[7]},生成元素[1],[3],[5],[7];

(b) {[0],[2],[4],[6]},生成元有[2],[6];

(c) {[0],[4]}=⟨[4]⟩;

(d) {[0]}=⟨[0]⟩.

2. ⟨[4],[6],[8]⟩有

$[0],[4],[6],[8],[6]-[4],[6]\boxplus[4],[6]\boxplus[6],[6]\boxplus[8],[8]\boxplus[8],[6]\boxplus[6]\boxplus[6],[8]\boxplus[8]\boxplus[4],[8]\boxplus[8]\boxplus[6]$. 它可以分别看成是[2],[10],[14],[22]生成的子群,把它记为 H. 因为采用加法记号,我们可以把幂写成倍,从而 H 的元素按生成元升幂排列

$$[0],[2],[4],[6],[8],[10],[12],[14],[16],$$

[18],[20],[22];

或者

[0],[10],[20],[6],[16],[2],[12],[22],[8],
[18],[4],[14];

或者

[0],[14],[4],[18],[8],[22],[12],[2],[16],
[6],[20],[10];

或者

[0],[22],[20],[18],[16],[14],[12],[10],[8],[6],[4],[2].

3. $\left(-\frac{1}{2}+\mathrm{i}\frac{\sqrt{3}}{2}\right)^2=-\frac{1}{2}-\mathrm{i}\frac{\sqrt{3}}{2}$, $\left(-\frac{1}{2}+\mathrm{i}\frac{\sqrt{3}}{2}\right)^3=1$.

4. 可以断言 $ab\neq e$. 否则 $ab=e$,则 $b=a^{-1}\in\langle a\rangle$,同时,在此条件下,必有 $ac=b$(因为 $ac\neq e$,再由消去律 $ac\neq a$, $ac\neq c$),于是 $c=a^{-1}b=a^{-2}\in\langle a\rangle$,从而 $G=\langle a\rangle$,矛盾.

同时,利用消去律又知 $ab\neq a$, $ab\neq b$. 故知 $ab=c$. G 的乘法表只有一种排法

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

习 题 五

1. 若 $(ab)^n=e$,即 $a(ba)\cdots(ba)b=e$,必有

$$(ba)\cdots(ba)(ba)=(ba)^n=e.$$

2. 对任意 $x\in G$,应有

$$(xax^{-1})^2=(xax^{-1})(xax^{-1})=xa^2x^{-1}=xex^{-1}=e,$$

即 xax^{-1} 的阶数只能为 1 或 2;也就是说,或者

$$xax^{-1}=e,\quad xa=x,\quad a=e$$

或者 xax^{-1} 阶数为 2, $xax^{-1}=a$,即

$$xa = ax.$$

前者与 a 之阶数为 2 矛盾，只能有 $xa = ax$.

3. 任取 $g,h\in H$. 由于 g,h 阶数有限，可设

$$g^m = e,\quad h^n = e.$$

于是 $(gh)^{mn} = g^{mn}h^{mn} = e$，$gh$ 的阶数有限，从而 $gh\in H$.

若 $g\in H$，$g^m = e$，那么 $(g^{-1})^m = (g^m)^{-1} = e$；从而 $g^{-1}\in H$.

4. 任取 $x,y\in G$，则 x,y,xy 的阶数不为 4，至多是 2. 故

$$x^2 = e,\quad y^2 = e,\quad (xy)^2 = e,$$

从而上述 3 元每个元素的逆元就是自己. 故

$$(xy)^{-1} = xy,\quad y^{-1}x^{-1} = xy,\quad yx = xy.$$

5. g 的阶数要整除 p^2，只能是 $1,p,p^2$. 若某元 g 之阶数为 p^2，则 G 为循环群，矛盾. 故对每个 $g\in G$ 恒有 $g^p = e$.

6. 若 $a\in H$，a 的阶数是无限的，则当 $r\neq s$ 时恒有 $a^r\neq a^s$. 故 $a\notin\langle a^2\rangle$.

同时，$a^2\neq e$，故 $\langle a^2\rangle\neq\{e\}$. 由题设，应有 $\langle a^2\rangle\supseteq H$. 这与 $a\in H$ 矛盾.

7. 6.

习 题 六

1.

	$(0^*,0^*)$	$(0^*,1^*)$	$(0^*,2^*)$	$(1^*,0^*)$	$(1^*,1^*)$	$(1^*,2^*)$
$(0^*,0^*)$	$(0^*,0^*)$	$(0^*,1^*)$	$(0^*,2^*)$	$(1^*,0^*)$	$(1^*,1^*)$	$(1^*,2^*)$
$(0^*,1^*)$	$(0^*,1^*)$	$(0^*,2^*)$	$(0^*,0^*)$	$(1^*,1^*)$	$(1^*,2^*)$	$(1^*,0^*)$
$(0^*,2^*)$	$(0^*,2^*)$	$(0^*,0^*)$	$(0^*,1^*)$	$(1^*,2^*)$	$(1^*,0^*)$	$(1^*,1^*)$
$(1^*,0^*)$	$(1^*,0^*)$	$(1^*,1^*)$	$(1^*,2^*)$	$(0^*,0^*)$	$(0^*,1^*)$	$(0^*,2^*)$
$(1^*,1^*)$	$(1^*,1^*)$	$(1^*,2^*)$	$(1^*,0)$	$(0^*,1^*)$	$(0^*,2^*)$	$(0^*,0^*)$
$(1^*,2^*)$	$(1^*,2^*)$	$(1^*,0^*)$	$(1^*,1^*)$	$(0^*,2^*)$	$(0^*,0^*)$	$(0^*,1^*)$

2. $(1^*,2^*)$.

3. $\{(\bar{0},\bar{0},\bar{0})\}$, $\mathbf{I}_2\otimes\mathbf{I}_2\otimes\mathbf{I}_2$, $\{\bar{0}\}\otimes\mathbf{I}_2\otimes\mathbf{I}_2$, $\mathbf{I}_2\otimes\{\bar{0}\}\otimes\mathbf{I}_2$, $\mathbf{I}_2\otimes\mathbf{I}_2\otimes\{0\}$, $\{\bar{0}\}\otimes\{\bar{0}\}\otimes\mathbf{I}_2$, $\{\bar{0}\}\otimes\mathbf{I}_2\otimes\{\bar{0}\}$, $\mathbf{I}_2\otimes\{\bar{0}\}\otimes\{\bar{0}\}$.

复 习 题

2. 由 $y^{-1}=x^{-1}yx$ 得

$$x^{-1}=y^{-1}xy=(x^{-1}yx)xy.$$

两端消去 x^{-1}，得 $yxxy=e$. 据逆元唯一性知

$$x^2y^2=e,\quad (y^{-1})^2=x^2.$$

再用 $x^{-1}yx$ 代替 y^{-1}，上面的右侧等式变成

$$(x^{-1}yx)^2=x^2,\quad x^{-1}y^2x=x^2.$$

从两端消去 x^{-1} 和 x 得 $y^2=x^2$. 又因为 $x^2y^2=e$，因此得 $x^4=e$，$y^4=e$.

3. 若 $ag=ah$，消去 a 得 $g=h$，这说明 f 是单射.

对任意 $h\in G$，我们有 $f(a^{-1}h)=a(a^{-1}h)=h$，这说明 f 是满射.

4. 应当首先解决合理性问题. 若 $a_1H=a_2H$，则 $a_2^{-1}a_1\in H$. 由于 H 是子群，故

$$(a_2^{-1}a_1)^{-1}=a_1^{-1}(a_2^{-1})^{-1}\in H.$$

从而 $Ha_1^{-1}=Ha_2^{-1}$；也就是说 σ 与 S 的元素（左陪集）的代表元选择无关.

5. 首先，$a=a^1$，$b=ba^0$，即 a 和 b 分别是这 3 种形式元素之一.

其次，任取 ba^j，b^2a^i，则

$$ba^j=baa^{j-1}=aba^{j-1}=a^jb.$$

故 $(ba^j)(b^2a^i)=b^3a^{j+i}$ 为 3 形式之一.

于是可以说明这 3 种形式元素的全体已经构成群，且等于 $\langle a,b\rangle$.

6. $\langle 2\rangle\subseteq H\subseteq\mathbf{I}$. 如果 $\langle 2\rangle\neq H$，即有奇数 $j\in H$，设 $j=2n+1$，$n\in\mathbf{I}$，那么由

$$j\in H,\quad 2n\in\langle 2\rangle\subseteq H$$

推出 $1=j-2n\in H$, $\mathbf{I}=H$ 矛盾.

9. 设 $G=\{a_1,a_2,\cdots,a_n\}$. 由消去律知

$$a_1\cdot a_1,\ a_1\cdot a_2,\ \cdots,\ a_1\cdot a_n$$

两两不同,它们是 G 的 n 个不同的元素. 而 G 只有 n 个元素,所以它们就是 G 的全部元素. 从而必有 i 使得 $a_1\cdot a_i=a_1$.

任取 $x\in G$,因为

$$a_1\cdot a_1,\ a_2\cdot a_1,\ \cdots,\ a_n\cdot a_1$$

乃是 G 之全部元素,故必有 $y\in G$ 使 $x=y\cdot a_1$. 于是

$$x\cdot a_i=(y\cdot a_1)\cdot a_i=y\cdot(a_1\cdot a_i)=y\cdot a_1=x.$$

由于 x 是任意的,这说明 a_i 就一个右恒等元.

同样,由于对任意 j,

$$a_j\cdot a_1,\ a_j\cdot a_2,\ \cdots,\ a_j\cdot a_n$$

是 G 之全部元素,必有 a_k 使得 $a_j\cdot a_k=a_i$,这说明每个 a_j 都有右逆元.

第三章　群　的　同　态

习　题　一

1. $f(xy)=axa^{-1}aya^{-1}=f(x)f(y)$.

对任意 $y\in G$,恒有

$$y=a(a^{-1}ya)a^{-1}=f(a^{-1}ya),$$

这说明 f 是满射. 群满足消去律,从而 f 是个单射.

4*. 首先,对任意 $x,y\in G$,由于由 x 导出的内自同构为恒等映射,必有 $xyx^{-1}=y$,也就是 $xy=yx$, G 为交换群.

其次,当 G 为交换群时,规定

$$f:x\to x^{-1},\ 对任意\ x\in G,$$

则 f 也是内自同构. 据题意 f 为恒等映射, 即 $x = x^{-1}$, $x^2 = e$, 对每个 $x \in G$ 都成立.

5. 设 f 是$(\mathbf{Q}, +)$到$(\mathbf{Q}, +)$的同构, $f(1) = a$. 那么, 对任意正整数 n, 由 n 等于 n 个 1 相加而 f 是同构映射, 故

$$f(n) = f(1 + \cdots + 1) = nf(1) = na.$$

对于负整数 $m = -n$, 有

$$f(m) = f(-n) = -f(n) = (-n)a = ma.$$

对正整数 n, 由于 $n \cdot \frac{1}{n} = 1$.

$$f(1) = f\left(n \cdot \frac{1}{n}\right) = f\left(\frac{1}{n} + \cdots + \frac{1}{n}\right) = nf\left(\frac{1}{n}\right),$$

即 $nf\left(\frac{1}{n}\right) = a$, 推出 $f\left(\frac{1}{n}\right) = \frac{1}{n}a$.

总结之就有, 对任意有理数$\frac{m}{n}$, 恒有

$$f\left(\frac{m}{n}\right) = mf\left(\frac{1}{n}\right) = \frac{m}{n} \cdot a,$$

f 是由 a 导出的映射.

6. 偶数加群$(E, +)$是整数加群的一个真子群, 而整数加群$(\mathbf{I}, +)$同构于$(E, +)$的真子群

$$K = \{4n \mid n \in \mathbf{I}\}.$$

习 题 二

1. 只要确定 1^* 在自同构之下的像, 则其他各元的像完全确定, 恒等映射 f 及

$$f_1(i^*) = 2i^*, \quad f_2(i^*) = 3i^*, \quad f_3(i^*) = 4i^*,$$

即$(\mathbf{I}_5, +)$的全部自同构.

2. A 是可逆的, 故 f 是双射, 又

$$f((a_1, \cdots, a_n) + (b_1, \cdots, b_n))$$
$$= ((a_1, \cdots, a_n) + (b_1, \cdots, b_n))A$$

$$=(a_1,\cdots,a_n)A+(b_1,\cdots,b_n)A$$
$$=f((a_1,\cdots,a_n))+f(b_1,\cdots,b_n)).$$

3. 设 $H=\{e,h\}$. 对任意 $g\in G$,由 H 之不变性 $ghg^{-1}\subseteq H$ 知
$$ghg^{-1}=h \text{ 或 } ghg^{-1}=e.$$
但 $ghg^{-1}=e$ 时蕴涵 $h=e$,所以只能有
$$ghg^{-1}=h,\quad gh=hg;$$
也就是 $h\in Z$.

5′. 任取 $x\in H$, $y\in K$,看
$$xyx^{-1}y^{-1}=(xyx^{-1})y^{-1},$$
由于 K 是 G 的不变子群,故 $xyx^{-1}\in K$,同时,$y^{-1}\in K$,从而
$$(xyx^{-1})y^{-1}\in K.$$

同理,
$$xyx^{-1}y^{-1}=x(yxy^{-1}),$$
而 $yxy^{-1}\in H$, $x\in H$,故 $xyx^{-1}y^{-1}\in H$.

所以 $xyx^{-1}y^{-1}\in H\cap K=\{e\}$. 进而 $xyx^{-1}y^{-1}=e$,也就是 $xy=yx$.

6. 该群的特点是 a,b,c 三个元素中任意两个相乘均得第三者,而每个元素自己乘自己得其本身.

若 σ 是 G 上可逆变换且 $\sigma(e)=e$,则 σ 必为自同构,只要在 $\sigma(xy)$ 计算中分别 x,y 相同与不同情形,恒有
$$\sigma(xy)=\sigma(x)\sigma(y).$$

而每个使 e 不动的可逆变换恰好就是 a,b,c 三个元素的一个置换,故 $\mathrm{Aut}(G)\approx \mathbf{S}_3$.

习 题 三

1. $g^{m+n}=g^m\cdot g^n$.

2. 当 g 之阶为 3 时,
$$\mathrm{Ker}(\sigma)=\{\cdots,-3,0,3,6,\cdots\}.$$
当 g 之阶无限时,$\mathrm{Ker}(\sigma)=\{0\}$.

3. 由于

$$L:(x,y,z)\to(x,y,z)\begin{pmatrix}1 & 2 & 1\\ 2 & 1 & 1\\ -1 & -1 & 2\end{pmatrix},$$

而矩阵乘法适合分配律故 L 是个同态映射.

而 L 的核就是方程组

$$\begin{cases}x+2y-z=0,\\ 2x+y+z=0,\\ x-y+2z=0\end{cases}$$

的解的集合,故 $\mathrm{Ker}(L)=\{(t,-t,-t)\mid t\in\mathbf{R}\}$.

4. 任取 $a+\mathrm{i}b\in\mathbf{C}^*$, $c+\mathrm{i}d\in\mathbf{C}^*$,其中 a,b 和 c,d 都是实数.那么,

$$\begin{aligned}&\sigma((a+\mathrm{i}b)(c+\mathrm{i}d))\\ &\quad=\sigma(ac-bd+\mathrm{i}(bc+ad))\\ &\quad=\sqrt{(ac-bd)^2+(bc+ad)^2} &&(\text{定义})\\ &\quad=\sqrt{a^2+b^2}\cdot\sqrt{c^2+d^2} &&(\text{算})\\ &\quad=\sigma(a+\mathrm{i}b)\sigma(c+\mathrm{i}d). &&(\text{定义})\end{aligned}$$

5*. 任取$(m,n)\in\mathbf{I}\times\mathbf{I}$, $(k,l)\in\mathbf{I}\times\mathbf{I}$,

$$\begin{aligned}&\sigma((m,n)+(k,l))\\ &\quad=\sigma((m+k,n+l)) &&(\mathbf{I}\times\mathbf{I}\text{ 中加法})\\ &\quad=(m+k)+(n+l) &&(\sigma\text{ 的定义})\\ &\quad=(m+n)+(k+l) &&(\text{数加的交换结合律})\\ &\quad=\sigma((m,n))+\sigma((k,l)). &&(\sigma\text{ 的定义})\end{aligned}$$

任意$(m,n)\in\mathrm{Ker}(\sigma)$充要条件是

$$\sigma((m,n))=m+n=0,$$

也就是 $m+n=0$, $n=-m$.故

$$\begin{aligned}\mathrm{Ker}(\sigma)&=\{(m,n)\in\mathbf{I}\times\mathbf{I}\mid n=-m\}\\ &=\{(m,-m)\mid m\in\mathbf{I}\}.\end{aligned}$$

习 题 四

1. §2 之例 7 表明 $\mathbf{S}_3$ 仅有一个非平凡的不变子群 $\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$. $\mathbf{S}_3$ 对这个不变子群的商群结构见本节例 1.

2. 用 G 代表克莱因四元数群,

$$G=\{\pm I,\pm A,\pm B,\pm C\}.$$

本章 §2 之例题 8 已经指明

$$H=\{I,-I\},\quad K=\{I,-I,A,-A\}$$
$$L=\{I,-I,B,-B\},\quad J=\{I,-I,C,-C\}$$

都是 G 的不平凡的不变子群.

商群 G/K 含两个元素,陪集

$$K=\{I,-I,A,-A\},$$
$$BK=\{B,-B,C,-C\}.$$

注意,$BK=(-B)K=CK=(-C)K$. 可排出 G/K 之乘法表(实际上,所有的二元群均同构).

	K	BK
K	K	BK
BK	BK	K

G/L 和 G/J 均与 G/K 结构相同.

而群 G/H 含 4 个元素,即陪集

$$H=\{I,-I\},\quad AH=\{A,-A\},$$
$$BH=\{B,-B\},\quad CH=\{C,-C\}.$$

其乘法表是

	H	AH	BH	CH
H	H	AH	BH	CH
AH	AH	H	CH	BH
BH	BH	CH	H	AH
CH	CH	BH	AH	H.

3. N 是 G 的不变子群是显然的.

建立群 G 到其子群 $K=\{5^m \mid m\in \mathbf{I}\}$ 的映射,

$$\sigma: 2^n5^m \to 5^m.$$

因为 G 中的有理数写成 2^n5^m 形式时 n 和 m 都有该数唯一确定(由整数分解唯一性知,若 $2^n5^m=2^l5^k$,必导致 $n=l$, $m=k$),从而上述对应是完全确定的.

又,对任意 $2^m5^n, 2^k5^l\in G$,

$$\begin{aligned}
&\sigma(2^m5^n\cdot 2^k5^l)\\
&\quad=\sigma(2^{m+k}\cdot 5^{n+l})\\
&\quad=5^{n+l} \qquad\qquad (\sigma\text{ 之定义})\\
&\quad=5^n\cdot 5^l\\
&\quad=\sigma(2^m5^n)\sigma(2^k5^l). \quad (\sigma\text{ 之定义})
\end{aligned}$$

从而 σ 是 G 到 K 的群同态映射. 任取 $5^n\in K$,则 $\sigma(5^n)=5^n$,这说明 σ 的满射.

现在来研究 σ 的核. 若 $2^m5^n\in G$,使

$$\sigma(2^m5^n)=5^n=1,$$

则 $2^m5^n=2^m$. 所以

$$\operatorname{Ker}(\sigma)=N.$$

由群同态基本定理,得 $G/N\cong K$.

4. 由于 $\mathbf{I}\times\mathbf{I}$ 到 $\mathbf{I}$ 的群同态

$$\sigma:(m,n)\to m+n$$

是满的, $\operatorname{Ker}(\sigma)=N$,所以由群同态基本定理可得 $(\mathbf{I}\times\mathbf{I})/N\cong\mathbf{I}$.

5. G/Z 为循环群,设 gZ 为 G/Z 的一个生成元, $g\in G$.

任取 $x\in G$, xZ 即为商群 G/Z 的一个元素,而 gZ 为生成元,必有 $n\in\mathbf{I}$ 使

$$(gZ)^n=g^nZ=xZ.$$

从而,必有 $z\in Z$ 使 $x=g^nz$.

任取 $y\in G$,又必有 $m\in\mathbf{I}$, $w\in Z$ 使得 $y=g^mw$.

于是

$$xy=(g^n z)(g^m w)=g^n g^m zw=g^m wg^n z=yx.$$

由于 x,y 是任意的,上式说明 G 是交换群.

复 习 题

1. 任取 $x\in H\cap K$ 及 $k\in K$,由于 $x\in H$, H 是 G 的不变子群,故 $kxk^{-1}\in K$. 又由于 $x\in K$, $k\in K$,故 $kxk^{-1}\in K$. 从而

$$kxk^{-1}\in H\cap K.$$

2. 每个 H_x 都是 G 的子群,所以它们的交集 K 必为 G 的子群.

现在,对任意 $k\in K$ 及 $g\in G$,我们来证明 $gkg^{-1}\in K$,也就是要证明,对任意 x,有 $gkg^{-1}\in H_x$.

事实上,$k\in K$,对于元素 $g^{-1}x$ 应有 $k\in H_{g^{-1}x}$;从而有 $h\in H$ 使

$$k=(g^{-1}x)h(g^{-1}x)^{-1}=g^{-1}xhx^{-1}g,$$

进而有 $gkg^{-1}=xhx^{-1}\in H_x$.

由 x 的任意性推出 $gkg^{-1}\in K=\bigcap\limits_{x\in G}H_x$. 再由 g 的任意性推出 K 是 G 的不变子群.

3. 任意 $x,y\in N$,由 $Hx=xH$, $Hy=yH$ 得

$$H(xy)=x(Hy)=x(yH)=(xy)H,$$

即知 $xy\in N$. 再由 $Hx=xH$ 得 $x^{-1}H=Hx^{-1}$ 知道 $x^{-1}\in N$. 所以,N 是 G 的子群.

对于 $h\in H$,当然有 $Hh=hH$,故 $H\subseteq N$.

任取 $x\in N$,恒有 $xH=Hx$,这说明 H 是 N 的不变子群.

4. 若 $y\in C$,那么,对任意 $h\in H$ 都有

$$hy=yh,$$

当然有,$Hy=yH$. 故 $C\subseteq N$,且容易验证 C 是 N 的子群.

进一步,对任意 $x\in N$, $y\in C$,我们来证明 $xyx^{-1}\in C$.

任取 $h\in H$,由于 $Hx=xH$,必有 $k\in H$ 使

$$hx = xk, \quad x^{-1}h = kx^{-1}.$$

于是有

$$\begin{aligned} & h(xyx^{-1}) \\ & = (hx)(yx^{-1}) && (\text{结合律}) \\ & = (xk)(yx^{-1}) && (hx = xk) \\ & = x(yk)x^{-1} && (y \in C) \\ & = xy(x^{-1}h) && (x^{-1}h = kx^{-1}). \end{aligned}$$

5. 在群 H 中 5^* 的周期是 4，而群 K 中 5^*，7^* 和 11^* 的周期均为 2，H 不同构于 K.

6. 计算 ij，jk 和 ki，对照两群之乘法表.

7. 先证明 σ 是单射. 若有 $x, y \in G$,

$$xf(x^{-1}) = yf(y^{-1}),$$

两端左乘 y^{-1}，右乘 $f(x)$，得

$$y^{-1}x = f(y^{-1})f(x) = f(y^{-1}x).$$

由所给条件知 $y^{-1}x = e$，$x = y$.

有限群上的变换只要是单射必然还是满射；从而为双射.

8. 令

$$\sigma: \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \to a + ib,$$

即得 $(G, +)$ 到 $(\mathbf{C}, +)$ 的同构映射.

再令

$$\tau: \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \to a + ib, \quad a^2 + b^2 \neq 0,$$

则得 $(G^{\#}, \cdot)$ 到 $(\mathbf{C}^{\#}, \cdot)$ 的映射. 容易看出，这是个双射.

进一步，任取

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \begin{pmatrix} c & d \\ -d & c \end{pmatrix}, \quad a^2 + b^2 \neq 0, \ c^2 + d^2 \neq 0,$$

都有

$$\tau\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix},\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right)$$

$$= \tau\left(\begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & ac-bd \end{pmatrix}\right)$$

$$= (ac-bd)+\mathrm{i}(ad+bc) \qquad (\tau \text{ 的定义})$$

$$= (a+\mathrm{i}b)(c+\mathrm{i}d) \qquad (\text{复数乘法})$$

$$= \tau\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right)\tau\left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right).$$

9. 因为$(xy)^n = x^n y^n$ 故也. 且 $\mathrm{Ker}(\sigma) = \{x \in G \mid x^n = e\}$.

10. 矩阵

$$A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \quad a \neq 0,\ d \neq 0$$

的逆矩阵是$\begin{pmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{pmatrix}$. 从而

$$A\begin{pmatrix} 1 & f \\ 0 & c \end{pmatrix}A^{-1} = \begin{pmatrix} 1 & x \\ 0 & c \end{pmatrix} \in K.$$

这里我们不需要算出 x 就足以说明问题.

令

$$\sigma: \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \to a, \quad a \neq 0,\ d \neq 0,$$

则得到 G 到非零实数乘法群$(\mathbf{R}^{\#},\cdot)$的一个映射. 显然是个满射. 计算 σ 的核,矩阵 $A \in G$ 属于 $\mathrm{Ker}(\sigma)$的充要条件是 $a=1$,也就是 $A \in K$,即

$$\mathrm{Ker}(\sigma) = K.$$

由群同态基本定理得 $G/K \approx (\mathbf{R}^{\#},\cdot)$.

11. 商群 $\mathbf{Q}/\mathbf{I}$ 的每个元素就是一个有理数$\frac{m}{n}$对 $\mathbf{I}$ 的陪集$\frac{m}{n}+\mathbf{I}$, $n \neq 0$.

不管$\frac{m}{n}$是正是负，我们总可以要求 $n>0$. 那么

$$n\left(\frac{m}{n}+\mathbf{I}\right)=\left(\frac{m}{n}+\cdots+\frac{m}{n}\right)+\mathbf{I}=m+\mathbf{I}=\mathbf{I}.$$

而 $\mathbf{I}$ 就是群 $\mathbf{Q}/\mathbf{I}$ 的零元.

所以，$\mathbf{Q}/\mathbf{I}$ 的每个元素的周期(阶数)都是有限的.

第四章　环与理想

习　题　一

2. 若 R 可换，对任意 $a,b\in R$ 有 $ab=ba$. 从而

$$(a+b)(a-b)=a^2+ba-ab-b^2=a^2-b^2.$$

反之，若对任意 $a,b\in R$ 恒有 $(a+b)(a-b)=a^2-b^2$，而由分配律知

$$(a+b)(a-b)=a^2+ba-ab-b^2,$$

故得 $ba-ab=0$，即 $ab=ba$. R 可换.

3. 要注意，按规定 $a-b$ 就是 $a+(-b)$，于是

$$\begin{aligned}(a-b)+(b-c)&=[a+(-b)]+[b+(-c)]\\&=a+[(-b)+b]+(-c).\end{aligned}$$

而 $(-b)+b=0$，故 $(a-b)+(b-c)=a+(-c)=a-c$.

4. 任取 $a\in R$，由 $e\cdot e=e$ 可得

$$x\cdot e\cdot e=x\cdot e,\quad (x\cdot e-x)\cdot e=0.$$

由于 e 不是零因子，$xe-x$ 只能等于 0，也就是 $x\cdot e=x$. 同理可知 $e\cdot x=x$. 由 x 的任意性知 e 为 R 的恒等元.

6. 若 R 是有 1 的交换环且满足消去律，那么 $ab=0$ 蕴涵 $a\cdot b=a\cdot 0$，导致 $b=0$.

7. 若 $(R,+,\cdot)$ 是有 5 个元素的环，那么 $(R,+)$ 是有 5 个元素的加法群. 由于 5 是素数，$(R,+)$ 必为循环群，可记为

$$R = \{0, a, a+a, a+a+a, a+a+a+a\}.$$

按已约定的符号,就是

$$R = \{0, a, 2a, 3a, 4a\}.$$

任取 R 中元素 ma, na,则

$$(ma)\cdot(na) = mn(a\cdot a).$$

由于 R 是个环 $a\cdot a \in R$,必有 $0 \leqslant k \leqslant 4$ 使 $a\cdot a = ka$. 从而 $(ma)\cdot(na) = mnka$. 同理 $(na)\cdot(ma) = mnka$.

习 题 二

1. 子环 $\{0^*, 2^*, 4^*\}$ 中 4^* 为恒等元,子环 $\{0^*, 3^*\}$ 中 3^* 是恒等元.

2. 若有理数

$$\frac{m}{n}, \quad \frac{k}{l}$$

是既约的,n 和 l 都与 p 互素,即 p 不能整除 n, l,则 p 亦不能整除 nl,从而 $\frac{m}{n} - \frac{k}{l}$ 通分后分母 nl 不能被 p 整除,既约后也不能被 p 整除,从而

$$\frac{m}{n} - \frac{k}{l} \in H.$$

同理,$\frac{m}{n}\cdot\frac{n}{l} = \frac{mn}{nl} \in H$.

3. 任取 $\frac{m}{n}, \frac{s}{t} \in K$, $m = p^k$, $t = p^l$,其中 k, l 是非负整数. 不妨设 $k \leqslant l$,则

$$\frac{m}{p^k} + \frac{s}{p^l} = \frac{mp^{l-k} + s}{p^l}, \quad \frac{m}{p^k}\cdot\frac{s}{p^l} = \frac{ms}{p^{k+l}}.$$

它们既约后分母仍为 p 的若干方(包含 p 的 0 方,分母为 1,此有理数为整数的情形).

4. $\{0\}, \{0, a\}, \{0, b\}, \{0, c\}, R$.

5. 若 $x, y\in S$,必有正整数 m, n 使 $mx=0$, $ny=0$,从而

$$mn(x+y)=n(mx)+m(ny)=0,$$

即 $x+y\in S$.

对任意 $r\in R$ 及 $x\in S$, $mx=0$,有

$$m(rx)=r(mx)=0,$$
$$m(xr)=(mx)r=0,$$

即 $rx, xr\in S$.

6. 先证 $f=e_1+e_2-e_1e_2$ 有如下性质

$$e_1f=e_1e_2+e_1e_2-e_1e_2=e_1,$$
$$e_2f=e_2e_1+e_2e_2-e_1e_2=e_2.$$

于是知 $f^2=(e_1+e_2)f=e_1+e_2=f$, f 为单方元.

由于 $f=e_1+e_2-e_1e_2\in(e_1,e_2)$,且

$$e_1=e_1f\in(f),\quad e_2=e_2f\in(f),$$

即知 $(f)=(e_1,e_2)$.

习 题 三

1. $\bar{\text{I}}$ 的单位有[1],[2],[4],[5],[7],[8];零因子有[0],[3],[6];周期为 3 的元素有[3]和[6];周期为 9 的有[1],[2],[4],[5],[7],[8]

2. 环 I/(16)的单位有[1],[3],[5],[7],[9],[11],[13],[15].若 I/(16)的子环 S 含上述元素之一,设为$[i]$,S 为子环,必含

$$[i]+[i]=[2i],$$

因为 $2i$ 是个偶数$[2i]$必为[0],[2],…,[14]中的一个,记为$[j]$.

由于 i 和 j 两数一奇一偶,必有整数 k, l 使 $li+kj=1$;从而

$$l[i]+k[j]=[1].$$

而 $l[i]$和 $k[j]$都在 S 中,故$[1]\in S$.从而 I/(16)的所有元素都在 S 中.

3. 对任意 $a\in R$，有

$$(e+I)(a+I)=ea+I=a+I=ae+I=(a+I)(e+I).$$

这说明 $e+I$ 是 R/I 的恒等元.

在偶数环 E 中，理想

$$(6)=\{\cdots,-6,0,6,\cdots\},$$

作商环 $E/(6)$.

E 是没有恒等元的环. 但商环

$$E/(6)=\{(6),2+(6),4+(6)\}$$

中，$4+(6)$是恒等元.

4. 整数环 $\mathbf{I}$ 为无零因子环，但商环 $\mathbf{I}/(4)$中$(2+(4))\cdot(2+(4))=(4)$，即 $2+(4)$是 $\mathbf{I}/(4)$的一个零因子.

所有形如

$$\begin{pmatrix} m & 0 \\ 0 & n \end{pmatrix}, \quad m,n\in \mathbf{I}$$

的矩阵在矩阵运算之下构成的环记为 R；所有形如

$$\begin{pmatrix} 0 & 0 \\ 0 & n \end{pmatrix}, \quad n\in I$$

的矩阵组成 R 的一个理想 I. 商环 R/I 的元素恒可由形如

$$\begin{pmatrix} m & 0 \\ 0 & 0 \end{pmatrix}, \quad m\in I$$

的矩阵作代表，可以看出 R/I 为无零因子环，但 R 中有很多零因子.

5. 任取 $r\in R$，由于 R/I 的元素加法周期有限必有正整数 m 使得

$$m(r+I)=mr+I=I,$$

也就是 $mr\in I$. 而 I 的每个元的加法周期有限，又必有正整数 t 使得 $t(mr)=0$，也就是$(tm)r=0$，r 的加法周期有限.

习 题 四

1.

$$\mathrm{Ker}(\sigma)=\left\{\begin{pmatrix}0 & c\\ 0 & 0\end{pmatrix}\middle|\ c\text{ 是实数}\right\},$$

$$\varphi^{-1}(\{A\})=\left\{\begin{pmatrix}1 & c\\ 0 & 0\end{pmatrix}\middle|\ c\text{ 是实数}\right\},$$

$$\varphi^{-1}(\{B\})=\left\{\begin{pmatrix}0 & c\\ 0 & \pi\end{pmatrix}\middle|\ c\text{ 是实数}\right\}.$$

2. 对于任意一个非零有理数 a,我们可使其分子与分母既约且分母大于零.设

$$a=m/n,\quad (m,n)=1,\quad n>0,$$

而且这种表法是由 a 唯一确定的.由于

$$f(na)=f(m)=g(m)=g(na),$$

而 f 和 g 都是同态映射,故

$$f(na)=f(a+\cdots+a)=nf(a)=ng(a).$$

两端同乘实数 $1/n$,即得 $f(a)=g(a)$.由 a 之任意性可推出 $f=g$.

3. 任取 $x,y\in f(S)$,必有 $s,t\in S$ 使得 $x=f(s)$, $y=f(t)$.从而

$$x-y=f(s)-f(t)=f(s+(-t))=f(s-t),$$
$$xy=f(s)f(t)=f(st).$$

由于 $s,t\in S$, S 是 R 的子环,故 $s-t$, $st\in S$.从而 $x-y$, $xy\in f(S)$.

4. f 实际上是 R 到 R/J 的自然同态限制在 I 上而已,f 是个环同态.

I 中元素 x 属于 $\mathrm{Ker}(f)$当而且仅当 $x+J=J$,也就是 $x\in J$, $x\in I\cap J$.故 $\mathrm{Ker}(f)=I\cap J$.

5. 由于对任意 $a+b\sqrt{3}, c+d\sqrt{3}\in T$ 有

$$f[(a+c)+(b+d)\sqrt{3}]=f(a+b\sqrt{3})+f(c+d\sqrt{3}),$$

而且

$$\begin{aligned} & f[(a+b\sqrt{3})(c+d\sqrt{3})] \\ & =f(ac+3bd+(ad+bc)\sqrt{3}) \qquad \text{(复数乘法)} \\ & =(ac+3bd)-(ad+bc)\sqrt{3} \qquad (f\text{ 的定义}) \\ & =(a-b\sqrt{3})(c-d\sqrt{3}) \qquad \text{(复数乘法)} \\ & =f(a+b\sqrt{3})f(c+d\sqrt{3}). \qquad (f\text{ 的定义}) \end{aligned}$$

任取 $a+b\sqrt{3}\in T$,则

$$f: a-b\sqrt{3}\rightarrow a+b\sqrt{3}.$$

所以,f 是满的,$\mathrm{Img}(f)=T$.

若 $a-b\sqrt{3}=c-d\sqrt{3}$,则

$$a-c=(b-d)\sqrt{3}, \qquad (*)$$

如果 $b-d\neq 0$,则有

$$\sqrt{3}=(a-c)/(b-d).$$

推出$\sqrt{3}$是有理数,矛盾.故 $b-d=0$,再由(*)推出 $a-c=0$,也就是

$$a=c, \quad b=d,$$

从而 $a+b\sqrt{3}=c+d\sqrt{3}$.这说明 f 是单射,$\mathrm{Ker}(f)=\{0\}$.

习 题 五

2. 任取$(r,s)\in R\oplus S$.由于 $r\in R$ 是周期有限的,必有正整数 m 使 $mr=0$.又由于 $s\in S$ 也是周期有限的,必有正整数 n 使得 $ns=0$.于是

$$mn(r,s)=(mnr,nms)=(0,0).$$

3. 任取$(r,s)\in R\oplus S$,必有正整数 m,n 使

$$r^m=0, \quad s^n=0.$$

从而$(r,s)^{mn}=(r^{mn},s^{mn})=(0,0)$.

4. $\mathrm{Ker}(f)=I\cap J$.

复 习 题

1. $\frac{1}{2}$在$(\mathbf{Q},+)$中生成的子群是

$$\{\frac{n}{2}\mid n\in\mathbf{I}\};$$

$\frac{1}{2}$在$(\mathbf{Q}-\{0\},\cdot)$生成的子群是

$$\{2^n\mid n\in\mathbf{I}\};$$

$\frac{1}{2}$在$(\mathbf{Q},+,\cdot)$生成的子环是

$$\{a_0(\frac{1}{2})^n+a_1(\frac{1}{2})^{n-1}+\cdots+a_n(\frac{1}{2})\mid n\in\mathbf{I},\ a_i\in\mathbf{I}\};$$

$\frac{1}{2}$在$(\mathbf{Q},+,\cdot)$生成的理想是$\mathbf{Q}$本身.

2. 由于环R是有1的交换环,所以它的任意一个元素$g(x)$生成的理想是

$$\{h(x)g(x)\mid h(x)\in R\}.$$

若$(2,x)$是由$g(x)$生成的,则必有$k(x),h(x)\in R$,

$$2=k(x)g(x),\qquad x=h(x)g(x).$$

使前式成立之$g(x)$只有$2,-2,1$和-1,使后式成立$g(x)$只能为$x,-x,1,-1$.但1和-1都不在$(2,x)$中,矛盾.

5*. 若$r_1,r_2\in T$,那么,对任意$x\in I$,

$$(r_1-r_2)x=r_1x-r_2x\in I.$$

而对任意$a\in R$及$r\in T$有

$$(ar)x=a(rx)\in I,\quad 对每\ x\in I,$$

这说明$ar\in T$.

6. 是子环.因为若$2m/n,2k/l\in S$,则

$$2m/n+2k/l=(2ml+2kn)/(nl),$$

其分母为奇数,分母为偶数,它们若有公因数并必为奇数,既约后,必然是分母为奇数,分子为偶数,从而 $2m/n+2k/l\in S$.

同理,$(2m/n)\cdot(2k/l)\in S$.

但 S 不是理想,因为 $2\in S$, $\frac{1}{2}\in\mathbf{Q}$,但 $1=2\cdot\frac{1}{2}\notin\mathbf{Q}$.

7. 商环 $\mathbf{I}/(p^2)$ 的单位有

$$1+(p^2),\cdots,(p-1)+(p^2),p+1+(p^2),\cdots,p(p-1)+1+(p^2).$$

而幂零元有 2 个,是

$$(p^2),P+(p^2),\cdots,(P-1)P+(p^2).$$

该环之非单位全幂零.

8. 只有一个非平凡理想 $\{(p^2),p+(p^2)\}$.

9. $4e=4e^2=(2e)(2e)$,而 R 无零因子,故由 $4e=0$ 推出 $2e=0$.

10. R 中的 $\{e,a,b\}$ 形成一个乘法群,进而是个 3 阶循环群,必有 $a^2=b$. 故乘法表是

$\cdot$	0	e	a	b
0	0	0	0	0
e	0	e	a	b
a	0	a	b	e
b	0	b	e	a

11. 由于 R 的阶数(作为加群)为 4,而 e 的周期必为 4 的因子,同时 $e+e=a\neq0$ 说明 e 的周期不为 a,所以 e 的周期只能是 4. 从而 $e+e+e=b$. 其加法表是

+	0	e	a	b
0	0	e	a	b
e	e	a	b	0
a	a	b	0	e
b	b	0	e	a

根据分配律,容易算出其乘法表

	0	e	$a=2e$	$b=3e$
0	0	0	0	0
e	0	e	a	b
$2e=a$	0	a	0	a
$3e=b$	0	b	a	e

12. 若有整数 m,n 使得 $m^2-3y^2=992$,那么,在自然同态下

$$m^2+(3)-(3n^2+(3))=992+(3),$$

$$m^2+(3)-(3)(n^2+(3))=2+(3).$$

由(3)是商环中的零元,它与任何元的积都是零,故得

$$m^2+(3)=2+(3),$$

$$(m+(3))(m+(3))=2+(3).$$

但 I/(3)中,$1+(3)$和$2+(3)$的平方都是$1+(3)$,绝没有元素的平方为$2+(3)$,矛盾.

13. 若有整数 m,n 使得

$$m^2-17y^2=855,$$

在 I 到 I/(17)的自然同态下,必有

$$(m+(17))(m+(17))=855+(17).$$

由于 $855=17\cdot 50+5$,故应有

$$(m+(17))^2=5+(17).$$

仔细计算商环 I/(17)各元素的平方,只有 $0+(17)$,$1+(17)$,$4+(17)$,$9+(17)$,$16+(17)$,$8+(17)$,$2+(17)$,$15+(17)$,$13+(17)$,绝不出现 $5+(17)$.

第五章　从环到域

习　题　一

1. 由于 $ab\neq 0$,故 $a\neq 0$.若 a 为零因子,有 $c\neq 0$,使 $ca=0$,

那么

$$c(ab)=(ca)b=0,$$

与 ab 不是零因子的假定相矛盾.

2. 若 σ 不是零同态,则必有 $\sigma(1)\neq 0$. 若不然,对任意 $a\in F$,

$$\sigma(a)=\sigma(a\cdot 1)=\sigma(a)\sigma(1)=0.$$

进一步,由于

$$\sigma(1)=\sigma(1\cdot 1)=\sigma(1)\sigma(1),\quad \sigma(1)\neq 0,$$

而 F' 是域,$\sigma(1)$ 必有逆,将上式两端同乘 $\sigma(1)$ 的逆,得 $\sigma(1)=1'$.

如果 F' 是个一般环,有恒等元 $1'$,不能保障 $\sigma(1)=1'$. 例如,F 是实数域,F' 是所有 2 阶方阵构成的矩阵环

$$\sigma: a\to\begin{pmatrix} a & 0\\ 0 & 0\end{pmatrix}$$

是 F 到 F' 的环同态映射,但 $\sigma(1)$ 不是 F' 的恒等元.

3. 由于 D 是交换的,该式等于

$$(d-a)(d-b)(d-c)=0.$$

而 D 无零因子,必有 $d-a=0, d-b=0$ 或者 $d-c=0$.

4. 设 F 是个 3 元域,它有零元 0 和恒等元 1,现将 F 记成 $\{0,1,a\}$. 由于 $(F,+)$ 是个 3 元群,必然是循环群,故知 $1+1=a$.

再据乘法分配律,可将 F 的乘法表完全确定出来

$\cdot$	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

5. 若 $(F,+,\cdot)$ 是 m 元域,那么 $(F-\{0\},\cdot)$ 就是 $m-1$ 元群. 由拉格朗日定理,对任意 $a\in F-\{0\}$ (也就是 $a\in F$, $a\neq 0$) 有 $a^{m-1}=1$. 当然有 $a^m=a$. 而 $a=0$ 也满足此式.

6. 对任意 $a+b\sqrt{-7}, c+d\sqrt{-7}\in R$,由于

$$(a+b\sqrt{-7})-(c+d\sqrt{-7})=(a-c)+(b-d)\sqrt{-7}\in R,$$

以及

$$(a+b\sqrt{-7})(c+d\sqrt{-7})=(ac-7bd)+(ad+bc)\sqrt{-7}\in R,$$

知道 R 是 $\mathbf{C}$ 的子环.

若$(a+b\sqrt{-7})\in R$,$(a+b\sqrt{-7})\neq 0$,则 $a\neq 0$, $b\neq 0$ 从而 $a^2+7b^2\neq 0$,所以

$$\frac{a}{a^2+7b^2},\quad \frac{b}{a^2+7b^2}$$

都是实数.从而

$$\frac{a}{a^2+7b^2}-\frac{b}{a^2+7b^2}\sqrt{-7}\in R.$$

而且

$$(a+b\sqrt{-7})\left(\frac{a}{a^2+7b^2}-\frac{b}{a^2+7b^2}\sqrt{-7}\right)=1.$$

这说明 R 的每个非零元均有逆.

习 题 二

1. 环 $\mathbf{I}/(p^2)$中

$$(p^2),p+(p^2),2p+(p^2),\cdots,(p-1)p+(p^2)$$

构成一个理想.它是该环的唯一的一个极大理想.

2. 设 I 为D 的素理想.若 $a,b\in D-I$,也就是 $a,b\notin I$,那么,因为 I 是D 的素理想,必有 $ab\notin I$,也就是 $ab\in D-I$. $D-I$ 在D 的乘法之下封闭.

设 $D-I$ 在D 的乘法之下封闭.若有 $a,b\in D$ 使得$ab\in I$,那么,必有 $a\in I$ 或者$b\in I$;若不然,由 $a,b\notin I$, $a,b\in D-I$ 可推出$ab\in D-I$,即 $ab\notin I$.

3. 若有 R 的理想 N 使得 $M\subset N\subset R$,设 $x\in N$, $x\notin M$.由于 x 必为单位,而 N 是理想,从而得 $x^{-1}x=1\in N$,对任意 $r\in R$ 有

$$r=r\cdot 1\in N.$$

4. 设 P 是R 的素理想.任取 $a',b'\in R'$,如果 $a'b'\in f(P)$,由于 f 是满的,必有 $a,b\in R$ 使得

$$f(a)=a', \quad f(b)=b'.$$

于是 $f(ab)=a'b'\in f(P)$. 即有 $r\in P$ 使

$$ab-r\in \mathrm{Ker}(f).$$

但 $\mathrm{Ker}(f)\subseteq P$,所以 $ab\in P$. 由于 P 是 R 的素理想,推知 $a\in P$ 或 $b\in P$,从而

$$a'=f(a)\in f(P) \text{或} \ b'=f(b)\in f(P).$$

设 P' 是 R' 的素理想. 任取 $a,b\in R$,如果 $ab\in f^{-1}(P')$,即 $f(ab)\in P'$,则由

$$f(a)f(b)=f(ab)\in P'$$

及 P' 是 R' 的素理想可推出 $f(a)\in P'$ 或者 $f(b)\in P'$,也就是

$$a\in f^{-1}(P') \text{或者} \ b\in f^{-1}(P').$$

5. 由于 $\{0\}$ 是 R 的素理想,由定义知 $R\neq\{0\}$,取 $x\in R$, $x\neq 0$,必有 $m>1$ 使得 $x^m=x$. 于是,对任意 $a\in R$ 有

$$x(x^{m-1}a-a)=x^m a-xa=(x^m-x)a=0.$$

但 $x\neq 0$, R 为素环,故有

$$x^{m-1}a-a=0, \quad \text{对所有} \ a\in R$$

这说明 x^{m-1} 是 R 的恒等元,记为 e.

对任意 $a\in R$, $a\neq 0$,必有 $n>1$ 使 $a^n=a$,那么,必有

$$a^n-a=a(a^{n-1}-e)=0.$$

而 $a\neq 0$,故 $a^{n-1}-e=0$, $a^{n-1}=e$. 由于 $n>1$, $n-1\geqslant 1$. 当 $n-1=1$ 时,说明 $a=e$, a 当然有逆,当 $n-1>1$ 时,有

$$e=a^{n-1}=a^{n-2}\cdot a,$$

此时 a 亦有逆元.

习 题 三

1. 按命题 1,在环 $(R,\#,\odot)$ 中,

$$(1,r)(1,s))=(1,s)(1,r)=(1,0),$$

逆元是唯一决定的.

2. 按定理 1,令

$$\sigma:\left\{\frac{a}{b}\right\}\to ab^{-1},\quad a,b\in R,\ b\neq 0.$$

则 σ 是环同态,是单的,又是满的.

3. 建立 R 的分式域 Q 到实数域的映射

$$\sigma:\left\{\frac{m+n\sqrt{2}}{p+q\sqrt{2}}\right\}\to\frac{m+n\sqrt{2}}{p+q\sqrt{2}},\quad p,q\neq 0,$$

后边的分号就是通常的实数的除法. 可以证明,σ 的定义是合理的,而且 σ 是R 的实数环R 的环同态映射,而且是单射.

σ 在R 中的像

$$S=\left\{\frac{m+n\sqrt{2}}{p+q\sqrt{2}}\mid m,n,p,q\in \mathbf{I},\ p,q\neq 0\right\}$$

是 R 的一个子域. 由于

$$\frac{m+n\sqrt{2}}{p+q\sqrt{2}}=\frac{mp-nq}{p^2-2q^2}+\frac{pn-mq}{p^2-2q^2}\sqrt{2},$$

即 S 中每个元均可写成$a+b\sqrt{2}$形式,其中 a,b 是有理数.

反过来,对任意有理数 a,b,设

$$a=m/n,\ b=p/q,\quad n,q\neq 0.$$

则

$$a+b\sqrt{2}=\frac{m}{n}+\frac{p}{q}\sqrt{2}=\frac{mq+np\sqrt{2}}{nq}\in S.$$

所以 $S=\{a+b\sqrt{2}\mid a,b$ 是有理数$\}$.

习 题 四

1. 计算多项式的系数.

2. H 是由 0 和 K 中所有 3 次多项式的首系数构成的集合. 若 $a,b\in H$, $a\neq 0$, $b\neq 0$,那么,必有

$$a_0+a_1x+a_2x^2+ax^3\in K,$$

$$b_0+b_1x+b_2x^2+bx^3\in K.$$

从而知

$$(a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+(a+b)x^3 \in K.$$

如果 $a+b=0$，显然已有 $a+b \in H$，如果 $a+b \neq 0$，那么，它就是上面的那个 K 中的三次多项式的首系数，亦有 $a+b \in H$.

3. $x+4^*, 0^*, x^2+3^*x+2^*, x^2+3^*x+2^*$.

4. $(2^*x+1^*)(2^*x+1^*)=1^*$.

5. 多项式 $f(x)-f(c)$，以 c 为其一根. 用命题 6.

6. 由于 $\sigma(f)(x)=f(x^2)$，我们任取 $F[x]$ 中两个多项式 $f(x), g(x)$，有

$$\sigma(f+g)(x)=(f+g)(x^2)=f(x^2)+g(x^2),$$

$$[\sigma(f)+\sigma(g)](x)=\sigma(f)(x)+\sigma(g)(x)=f(x^2)+g(x^2),$$

即 $\sigma(f+g)=\sigma(f)+\sigma(g)$.

同样也有

$$\sigma(fg)(x)=(fg)(x^2)=f(x^2)g(x^2)=[\sigma(f)(x)][\sigma(g)(x)],$$

也就是 $\sigma(fg)=\sigma(f)\sigma(g)$.

7. 设

$$f(x)=a_0+a_1x+\cdots+a_nx^n,$$

$$g(x)=b_0+b_1x+\cdots+b_mx^m,$$

那么，我们配上些 0，可认为 $m=n$.

$$\begin{aligned}\varphi(f(x)+g(x)) &= \varphi[(a_0+b_0)+\cdots+(a_n+b_n)x^n] \\ &= \sigma(a_0+b_0)+\cdots+\sigma(a_n+b_n)x^n \\ &= [\sigma(a_0)+\cdots+\sigma(a_n)x^n] \\ &\quad +[\sigma(b_0)+\cdots+\sigma(b_n)x^n] \\ &= \varphi[f(x)]+\varphi[g(x)].\end{aligned}$$

同理，$\varphi[f(x)g(x)]=\varphi[f(x)]\varphi[g(x)]$.

$R[x]$ 的多项式

$$f(x)=a_0+a_1x+\cdots+a_nx^n \in \mathrm{Ker}(\varphi)$$

的充要条件是其所有系数 $a_0, \cdots, a_n \in \mathrm{Ker}(\sigma)$.

习 题 五

1. 用 e 代表 F 的恒等元，可以证明，F 的每个非零元素 a 的（加法）周期与 e 的周期相同.

若有正整数 n 使得 $ne=0$，那么

$$na=n(ea)=(ne)\cdot a=0.$$

若有正整数 m 使得 $ma=0$，那么由

$$m(ea)=(me)a=0$$

及 $a\neq 0$ 知 $me=0$.

2. 域的特征数与其恒等元的加法周期相同，域与其每个子域有相同的恒等元.

3. 若 σ 是域 F 的自同构，e 是 F 的恒等元，那么必有

$$\sigma(e)=e,\quad \sigma(0)=0,$$

但 P 是由 e 和 0 生成的，σ 不变 e 和 0 则必不变 P 中任何元素.

复 习 题

1. 若 $x,y\in P(I)$，必有正整数 m,n 使

$$x^n,y^m\in I.$$

从而

$$(x-y)^{m+n}=x^{m+n}-mx^{m+n-1}y+\cdots+(-1)^{m+n}y^{m+n}.$$

上面等式右端每个加项中或者 x 的方次大于等于 n 或 y 的方次大于等于 m，从而每项都在 I 中，进而知 $x-y\in P(I)$.

对任意 $r\in R$ 及 $x\in P(I)$，设 $x^n\in I$，那么

$$(rx)^n=r^nx^n\in I,$$

从而知 $rx\in P(I)$，$P(I)$是 R 的理想.

由于 $I^2\subseteq I$，故 $P(I^2)\subseteq P(I)$. 反之，若 $x\in P(I)$，有正整数 n 使得 $x^n\in I$，那么 $x^{2n}\in I\cdot I$，因而 $x\in P(I^2)$，即知 $P(I)\subseteq P(I^2)$.

如果 I 是环 R 的素理想，当 $x\in P(I)$时，设正整数 n 使 $x^n\in$

I,那么,由 I 的素性,必有 $x \in I$.这意味着 $P(I) \subseteq I$.而 $I \subseteq P(I)$ 是显然的.

2. R 和 $R[x]$的特征数都等于恒等元的加法周期.

3. 由于 $a_0 = f(0)$,据§4之命题2

$$\sigma: f(x) \to f(0)$$

是个环同态映射.$f(x) \in \mathrm{Ker}(\sigma)$的充要条件是 $f(0) = a_0 = 0$.当 $f(x)$之常数项为0时,各项的 x 可以提出来写成

$$f(x) = g(x)x, \quad g(x) \in R[x].$$

这说明 $f(x) \in \mathrm{Ker}(\sigma)$的充要条件是 $f(x)$属于 x 生成的理想 (x).所以 $\mathrm{Ker}(\sigma) = (x)$.

由于 σ 是个满射,由环同态的基本定理

$$R[x]/\mathrm{Ker}(\sigma) \cong R.$$

4. $x^9 - x$.

5. $f(x) \in (g(x))$则必有 $h(x) \in F[x]$使

$$f(x) = g(x)h(x),$$

从而 $\deg(g(x)) \leqslant \deg(f(x))$.反过来还有

$$\deg(f(x)) \leqslant \deg(g(x)).$$

6*. 由于

$$\sigma_{a,b} \cdot \sigma_{c,d}: x \to a(cx+d)+b,$$

故 $\sigma_{a,b}\sigma_{c,d} = \sigma_{ac,ad+b} \in G$.再由

$$\sigma_{c^{-1},-c^{-1}d}\sigma_{c,d} = \sigma_{e,0},$$

知 $\sigma_{c,d}$的逆亦在G 中.G 是F 上变换群的一个子群.

规定

$$\varphi: \sigma_{a,b} \to a, \quad \sigma_{a,b} \in G,$$

则得到 G 到F 的一个满射.容易验证,这是个环同态,由环同态基本定理知

$$G/\mathrm{Ker}(\varphi) \cong F.$$

计算 $\mathrm{Ker}(\varphi)$,$\sigma_{a,b} \in \mathrm{Ker}(\varphi)$当而且仅当 $a = e$,故知 $\mathrm{Ker}(\varphi) = K$.

从而知道 $G/K\cong F$.

7. 由§1之命题1知含有限个元素的整环必为域. 若 F 为6元域,它的5个非零元构成一个乘法群,5是个素数,这个乘法群必然是循环群. 从而可把 F 的元素列出来,写成

$$F=\{0,1,a,a^2,a^3,a^4\}.$$

看 F 的元素 $1+a$,它显然不能等于1,也不能等于 a. 若 $1+a=0$,即 $a=-1$,则推出 $a^2=1$,与 a 的乘法周期为5矛盾.

若 $1+a=a^2$,那么由

$$(1+a)^5=1+a^5=(a^2)^5=1,$$

推出 $a^5=0$,矛盾. 同样 $1+a\neq a^3$, $1+a\neq a^4$.

这说明不存在6个元素的整环.

8. 看 x 和 y^2 生成的理想 (x,y^2),有

$$(x)\subseteq(x,y^2),$$

同时 $y^2\in(x,y^2)$,但 $y^2\notin(x)$; $y\in\mathbf{Q}[x,y]$,但 $y\in(x,y^2)$,故

$$(x)\subset(x,y^2)\subset\mathbf{Q}[x,y].$$

(x)不是 $\mathbf{Q}[x,y]$的极大理想.

第六章 因子分解理论

习 题 一

1. 单位有 $1^*,2^*,3^*,4^*$;相伴元有

2^*x^3+x; $4^*x^3+2^*x$; x^3+3^*x; $3^*x^3+4^*x$.

2. 若 x^3+x+1^* 不是 $\mathbf{I}_2[x]$的不可约元,设 $f(x)=x^3+x+1^*=g(x)h(x)$,因为 $g(x)$不是零多项式,它的次数只能是1,2,3次和0次. 若 $g(x)$是0次,它是常数多项式,而 $\mathbf{I}_2[x]$的常数多项式只有一个就是1,是个单位,说明 $g(x)$不是非平凡因子;若 $g(x)$是1次多项式,由于 $\mathbf{I}_2[x]$只有2个一次多项式

$$x,\quad x+1^*,$$

由于 $f(0^*)=1^*\neq 0$，故 $x\nmid f(x)$. 再由 $f(1^*)=1^*\neq 0$，又知 $(x+1^*)\nmid f(x)$. 这说明 $f(x)$ 没有 1 次的非平凡因子. 进而它也不能有二次的非平凡因子.

3. 在环 $\mathbf{I}[\sqrt{-2}]$ 中，5 是不可约的. 可以仿照例 5 定义 $\mathbf{I}[\sqrt{-2}]$ 到 $\mathbf{I}$ 的映射

$$\varphi: a+b\sqrt{-2}\to a^2+2b^2.$$

如果有 $a,b,c,d\in\mathbf{I}$ 使

$$5=(a+b\sqrt{-2})(c+d\sqrt{-2}),$$

那么必有

$$25=(a^2+2b^2)(c^2+2d^2).$$

若整数 a^2+2b^2 与 5 相伴（在整数环 $\mathbf{I}$ 中），必有 $a^2+2b^2=5$，矛盾. 所以

$$a^2+2b^2=1 \text{ 或 } c^2+2d^2=1.$$

也就是 $a+b\sqrt{-2}=\pm 1$ 与 5 相伴，或者 $c+d\sqrt{-2}=\pm 1$ 与 5 相伴.

4. 若 $a=b$，则 $x-a$ 就是 $x-a$ 与 $x-b$ 的最大公因子.

若 $a\neq b$，由于 $x-a$，$x-b$ 都是一次的，它们的公因子只能是一次的或常数多项式. 若

$$(cx+d)\mid(x-a),(cx+d)\mid(x-b),\quad c\neq 0,$$

则 $cx+d$ 与 $x-a$ 同为一次多项式，是相伴的. 同理 $cx+d$ 与 $x-b$ 相伴，最后导致 $x-a$ 与 $x-b$ 相伴. 用长除法得 $a=b$.

6. 如果整除关系在 $D-\{0\}$ 上是个等价关系. 用 e 代表 D 的恒等元，任取 $a\in D$，$a\neq 0$，由于 $e\mid a$，而整除是等价的，必有 $a\mid e$，a 为单位.

7. 若 $x\mid y$，有 $y=ux$，从而 $y\in(x)$，$(y)\subseteq(x)$；若 $(y)\subseteq(x)$，则 $y\in(x)$，有 $u\in D$ 使得 $y=ux$，$x\mid y$.

x 和 y 相伴的充分必要条件是 $x\mid y$ 且 $y\mid x$，利用上款，又得充要条件 $(x)\subseteq(y)$，$(y)\subseteq(x)$.

若 y 是 x 的非平凡因子，y 是 x 的因子，故 $(x)\subseteq(y)$；y 与 x 不相伴，故 $(x)\neq(y)$；从而有 $(x)\subset(y)$. 而 $(y)=D$ 则意味着 y 是单位，矛盾. 总之，$(x)\subset(y)\subset D$.

反之，$(x)\subset(y)$，则 $y|x$. 但 y 不与 x 相伴，而 $(y)\subset D$ 意味着 y 不是单位，所以，y 是 x 的非平凡因子.

习 题 二

1. $x+4^*$

2. 因为 a,b 互素，必有 $e,d\in D$ 使

$$ae+bd=1,$$

两端同乘 c，得

$$aec+bcd=c,$$

由于 $a|(aec)$ 和 $a|(bcd)$ 知 $a|c$.

3*. 设 I 是环 S 的一个理想，那么 $f^{-1}(I)$ 就是环 R 的一个理想. 由于 R 是主理想环，必有 $r\in R$ 使 $f^{-1}(I)=(r)$.

任取 $x\in I$，由于 f 是满的，必有 $a\in R$ 使 $f(a)=x$，由于 $a\in f^{-1}(I)$，知有 $c\in R$ 使 $a=cr$. 于是

$$x=f(a)=f(cr)=f(c)f(r)\in(f(r)).$$

所以 $I\subseteq(f(r))$. 反过来，又因为 $r\in f^{-1}(I)$，$f(r)\in I$ 知 $(f(x))\subseteq I$. 这说明，I 是由 $f(r)$ 生成的. 由 I 的任意性即知 S 是主理想环.

4. $1,-1,\mathrm{i},-\mathrm{i}$.

5. 看复数 $-1+3\mathrm{i}$ 的模数的平方 $1+3^2=10$，若复数 $a+\mathrm{i}b\in G$ 是 $-1+3\mathrm{i}$ 的非平凡因子，那么 a^2+b^2 必然整除 10，只能是 2 或 5，得

$$-1+3\mathrm{i}=(1+\mathrm{i})(1+2\mathrm{i}).$$

再看两个因子的模数，可断言 $1+\mathrm{i}$ 和 $1+2\mathrm{i}$ 在 G 中都是素的.

6. 若 a 是单位，由 $d(b)=d(a)$，可知 b 整除 D 的每个元素，从而 b 亦为单位，a 与 b 相伴.

若 a 不是单位且 a 与 b 不是相伴的，则与命题 3 矛盾.

习 题 三

2. 设

$$g(x)=a_nx^n+\cdots+a_1x+a_0,$$
$$h(x)=b_mx^m+\cdots+b_1x+b_0,$$

那么 $pf(x)$ 的系数，按降幂排起来乃是

a_nb_m,

$a_nb_{m-1}+a_{n-1}b_m$,

$a_nb_{m-2}+a_{n-1}b_{m-1}+a_{n-2}b_m$,

$\cdots$,

a_0b_0.

由于 $p\nmid a_n$，知 $p\mid b_m$. 又由 $p\mid(a_nb_{m-1}+a_{n-1}b_m)$ 及 $p\mid b_m$ 知 $p\mid(a_nb_{m-1})$，$p\mid b_{m-1}$，继续下去，即知 $p\mid b_0$.

复 习 题

1. $x^2+1^*=(x+2^*)(x+3^*)$.

2. x^2+x+1^* 是其一个最大公因子.

$x(x^5+x^4+1^*)+(x+1)(x^5+x+1^*)=x^2+x+1^*$.

4. 若 $d|a$, $d|b$ 则 $d|r$，从而 $d|a$ 且 $d|b$ 蕴涵 $d|b$, $d|r$. 反之亦然.

第七章 域的扩张

习 题 一

1. $x, x-3, x^2-2, x^2+1, x^2+1$.

2. 若 a 为 F 上的代数元，设 $p(x)\in F[x]$ 是 a 的极小多项

式，则 $p(x)$ 为不可约多项式. 对任意 $f(x)\in F[x]$，如果 $f(a)\neq 0$，由于 $p(x)$，$f(x)$ 互素，必有 $g(x)$，$h(x)$ 使

$$f(x)g(x)+h(x)p(x)=1.$$

于是知

$$f(a)g(a)+h(a)p(a)=f(a)g(a)=1,$$

这说明 $F[a]$ 的每个非零元均有逆，$F[a]$ 为域. 从而 $F[a]=F(a)$.

若 $F[a]=F(a)$，$F[a]$ 为域，必有 $f(x)\in F[x]$ 使得 $f(a)$ 是 a 的逆元，即

$$f(a)a=1,$$

也就是 a 满足多项式 $f(x)x-1$.

3. 可以断言 $\mathbf{Q}(\sqrt{2},\sqrt[3]{2})=\mathbf{Q}(\sqrt[6]{2})$.

首先，$2^{\frac{1}{6}}=2^{\frac{1}{2}}\cdot 2^{\frac{2}{3}}\cdot 2^{-1}$，而 $2^{\frac{1}{2}}=\sqrt{2}$，$2^{\frac{2}{3}}=(\sqrt[3]{2})^2$ 及 2^{-1} 都在域 $\mathbf{Q}(\sqrt{2},\sqrt[3]{2})$ 中，所以 $2^{\frac{1}{6}}=\sqrt[6]{2}$ 也在 $\mathbf{Q}(\sqrt{2},\sqrt[3]{2})$ 中；从而 $\mathbf{Q}(\sqrt[6]{2})\subseteq \mathbf{Q}(\sqrt{2},\sqrt[3]{2})$.

反过来，由于

$$2^{\frac{1}{2}}=(2^{\frac{1}{6}})^3,\quad 2^{\frac{1}{3}}=(2^{\frac{1}{6}})^2,$$

而 $\mathbf{Q}(\sqrt[6]{2})$ 是个域，所以 $\sqrt{2}$，$\sqrt[3]{2}$ 均在 $\mathbf{Q}(\sqrt[6]{2})$ 中；从而

$$\mathbf{Q}(\sqrt{2},\sqrt[3]{2})\subseteq \mathbf{Q}(\sqrt[6]{2}).$$

总之，即 $\mathbf{Q}(\sqrt{2},\sqrt[3]{2})=\mathbf{Q}(\sqrt[6]{2})$.

习　题　二

1. 一方面 $\sqrt{2}+\mathrm{i}\in \mathbf{Q}(\sqrt{2},\mathrm{i})$，从而

$$\mathbf{Q}(\sqrt{2}+\mathrm{i})\subseteq \mathbf{Q}(\sqrt{2},\mathrm{i}).$$

另一方面，$\mathbf{Q}(\sqrt{2}+\mathrm{i})$ 是个域，从而

$$\frac{1}{3}(\sqrt{2}+\mathrm{i})^{-1}=\sqrt{2}-\mathrm{i}\in \mathbf{Q}(\sqrt{2}+\mathrm{i}).$$

进而推出

$$\frac{1}{2}[(\sqrt{2}+\mathrm{i})+(\sqrt{2}-\mathrm{i})]=\sqrt{2}\in\mathbf{Q}(\sqrt{2}+\mathrm{i}).$$

同理知 $\mathrm{i}\in\mathbf{Q}(\sqrt{2}+\mathrm{i})$,故

$$\mathbf{Q}(\sqrt{2},\mathrm{i})\subseteq\mathbf{Q}(\sqrt{2}+\mathrm{i}),$$

最后得到 $\mathbf{Q}(\sqrt{2},\mathrm{i})=\mathbf{Q}(\sqrt{2}+\mathrm{i})$.

又因为 $\mathbf{Q}(\sqrt{2},\mathrm{i})=\mathbf{Q}(\sqrt{2})(\mathrm{i})$,而 $1,\sqrt{2}$,是 $\mathbf{Q}(\sqrt{2})$在 $\mathbf{Q}$ 上的基底,$1,\mathrm{i}$ 是 $\mathbf{Q}(\sqrt{2})(\mathrm{i})$在 $\mathbf{Q}(\sqrt{2})$上的一组基,故

$$1,\mathrm{i},\mathrm{i}\sqrt{2},\sqrt{2}$$

是 $\mathbf{Q}(\sqrt{2},\mathrm{i})$在 $\mathbf{Q}$ 上的一组基底.

2. 任取 $a\in K,a\notin F$,则

$$F\subseteq F(a)\subseteq K,$$

而且$[F(a):F]\mid[K:F]=p$.由于 p 与素数且 $F(a)\neq F$,即$[F(a):F]\neq 1$,知$[F(a):F]=p$;也就是 $K=F(a)$,K 为单纯扩张.

3. 若 $a\in K$, $f(a)=0$,那么,由

$$F\subseteq F(a)\subseteq K$$

即知$[F(a):F]$必然整除$[K:F]$.

另一方面,$f(x)$是 F 上的不可约多项式,a 满足 $f(x)$,则$[F(a):F]$等于 $f(x)$在 F 上的次数 m.所以得到 $m\mid n$.这说明 m 和 n 的最大公因子是 m.

但是,m 和 n 是互素的,从而必有 $m=1$,这与 $f(x)$在 F 上不可约矛盾.

4. 因为$\sqrt{3}=\left(\sqrt{2+\sqrt{3}}\right)^2-2\in\mathbf{Q}\left(\sqrt{2+\sqrt{3}}\right)$,故

$$\begin{aligned}\mathbf{Q}\left(\sqrt{2+\sqrt{3}}\right)&=\mathbf{Q}(\sqrt{3})\left(\sqrt{2+\sqrt{3}}\right)\\&=\mathbf{Q}\left(\sqrt{3},\sqrt{2+\sqrt{3}}\right).\end{aligned}$$

从而

$$\left[\mathbf{Q}\left(\sqrt{2+\sqrt{3}}\right):\mathbf{Q}\right]$$
$$=\left[\mathbf{Q}(\sqrt{3})\left(\sqrt{2+\sqrt{3}}\right):\mathbf{Q}(\sqrt{3})\right]\left[\mathbf{Q}(\sqrt{3}):\mathbf{Q}\right].$$

而

$$\left[\mathbf{Q}(\sqrt{3})\left(\sqrt{2+\sqrt{3}}\right):\mathbf{Q}(\sqrt{3})\right]=2,\quad \left[\mathbf{Q}(\sqrt{3}):\mathbf{Q}\right]=2,$$

所以$\left[\mathbf{Q}\left(\sqrt{2+\sqrt{3}}\right):\mathbf{Q}\right]=4$.

习　题　三

1. L 中的每一个元素都是由 G 中有限多个元素与 E 中有限多个元素加、减、乘、除得到的. 由于 G 中这些元素都是 F 上的代数元, E 中这些元素也都是 F 上的代数元,从而,据命题 2,它们组合成的 L 的元素也是 F 上的代数元.

2. 由于 F 之特征数为 p,故对任意 $a,b\in F$,

$$\sigma(a+b)=(a+b)^p=a^p+b^p=\sigma(a)+\sigma(b),$$
$$\sigma(ab)=(ab)^p=a^pb^p=\sigma(a)\sigma(b).$$

这说明 σ 是域 F 到自己的(环的)同态.

由于 $\sigma(1)=1\neq0$,知 $\mathrm{Ker}(\sigma)\neq F$,从而 $\mathrm{Ker}(\sigma)=\{0\}$. 这说明 σ 是个单射. 再由 F 的有限性知道其上的每个单射都是满的,最后就证明了 σ 是个自同构映射.

对任意 $b\in F$,由于 σ 是满的,故必有 $a\in F$ 使得 $b=\sigma(a)=a^p$. 又由于 σ 是单的,进而知这个 a 是由 b 唯一确定的.

3. a 是 K 上的代数元,那么 $K(a)$ 是 K 的有限扩张. 从而 $K(a)$ 是 K 的代数扩张. 据定理 1 知 $K(a)$ 必为 F 的代数扩张,特别地, a 应当是 F 上的代数元.

习　题　四

1. 若 $f(\alpha)=0$,那么

$$(\alpha^2-2)^3-3(\alpha^2-2)+1$$

$$
\begin{aligned}
&= \alpha^6 - 6\alpha^4 + 12\alpha^2 - 8 - 3\alpha^2 + 6 + 1 \\
&= \alpha^6 - 6\alpha^4 + 9\alpha^2 - 1 \\
&= (\alpha^3 - 3\alpha - 1)(\alpha^3 - 3\alpha + 1) \\
&= 0.
\end{aligned}
$$

这说明 $\alpha^2 - 2$ 是 $f(x)$的一个根. 同理可验证出 $2 - \alpha - \alpha^2$ 是$f(x)$的另一个根.

当然也可以直接计算,在 **C** 上有

$$
\begin{aligned}
&(x-\alpha)(x-\alpha^2+2)(x+\alpha^2+\alpha-2) \\
&= x^3 + (-\alpha-\alpha^2+2+\alpha^2+\alpha-2)x^2 \\
&\quad + (-\alpha^4-\alpha^3+2\alpha^2-\alpha^3-\alpha^2+2\alpha+2\alpha^2+2\alpha \\
&\quad -4+\alpha-1)x + \alpha^3+\alpha^2-2\alpha-\alpha^2+2 \\
&= x^3 + (-\alpha^4-2\alpha^3+3\alpha^2+5\alpha-5)x + 1.
\end{aligned}
$$

把 α^4 用 $\alpha(3\alpha-1)$替之(因为 $\alpha^3 = 3\alpha - 1$),知

$$
\begin{aligned}
&-\alpha^4 - 2\alpha^3 + 3\alpha^2 + 5\alpha - 5 \\
&= -\alpha(3\alpha-1) - 2(3\alpha-1) + 3\alpha^2 + 5\alpha - 5 \\
&= -3\alpha^2 + \alpha - 6\alpha + 2 + 3\alpha^2 + 5\alpha - 5 \\
&= -3.
\end{aligned}
$$

从而知 $f(x) = (x-\alpha)(x-\alpha^2+2)(x+\alpha^2-\alpha-2)$.

据此可知,$f(x)$在 $\mathbf{Q}(\alpha)$上可分解成一次式连乘积. 而 $1, \alpha, \alpha^2$ 是 $\mathbf{Q}(\alpha)$在 $\mathbf{Q}$ 上的基底,即$[\mathbf{Q}(\alpha):\mathbf{Q}] = 3$,不可能有 $\mathbf{Q}$ 的真扩张含在 $\mathbf{Q}(\alpha)$中. 所以 $\mathbf{Q}(\alpha)$即为 $f(x)$的分裂域.

2. 设有限域 F 有 n 个元素

$$
F = \{a_1, a_2 \cdots, a_n\}, \quad a_1 \neq 0.
$$

看 F 上的多项式

$$
f(x) = (x-a_1)(x-a_2)\cdots(x-a_n) + a_1.
$$

由于对每个元素 a_i 而言恒有

$$
f(a_i) = a_1 \neq 0,
$$

即 $f(x)$在 F 上没有根,从而 $f(x)$不能在 F 上分解成一次式的连乘积,F 不是代数封闭域.

3. 设 E 是 G 的一个代数扩张，任取 $b\in E$，则 $G(b)$ 是 G 的一个代数扩张，而 G 又是 $\mathbf{Q}$ 的代数扩张. 据§3之定理1知 $G(b)$ 是 $\mathbf{Q}$ 的一个代数扩张，即 $G(b)$ 的每个元素都是 $\mathbf{Q}$ 上的代数元；特别地，b 是 $\mathbf{Q}$ 上的代数元，由 G 的定义知 $b\in G$，再由 b 的任意性知 $E\subseteq G$，进而得 $E=G$. G 是代数封闭域.

复 习 题

1. 因为 $\sqrt[3]{2}$ 在有理数域 $\mathbf{Q}$ 上的极小多项式是 x^3-2，故 $\mathbf{Q}(\sqrt[3]{2})$ 中元素形如

$$a+b\sqrt[3]{2}+c\sqrt[3]{4},\quad a,b,c\in\mathbf{Q}.$$

设

$$(1+\sqrt[3]{2}+\sqrt[3]{4})(a+b\sqrt[3]{2}+c\sqrt[3]{4})=1,$$

由于 $1,\sqrt[3]{2},\sqrt[3]{4}$ 在 $\mathbf{Q}$ 上线性无关，必须有

$$a+2b+2c=1,$$
$$a+b+2c=0,$$
$$a+b+c=0.$$

从而推出 $c=0$, $b=1$, $a=-1$. 这说明 $-1+\sqrt[3]{2}$ 是 $1+\sqrt[3]{2}+\sqrt[3]{4}$ 的逆.

2. 由于 $\sqrt{5}\in\mathbf{Q}(\sqrt{5})$，$1\in\mathbf{Q}(\sqrt{5})$，故 $1+\sqrt{5}\in\mathbf{Q}(\sqrt{5})$，$\mathbf{Q}(1+\sqrt{5})\subseteq\mathbf{Q}(\sqrt{5})$. 反之，由于 $-1\in\mathbf{Q}(1+\sqrt{5})$，可推出 $-1+1+\sqrt{5}=\sqrt{5}\in\mathbf{Q}(1+\sqrt{5})$，

$$\mathbf{Q}(\sqrt{5})\subseteq\mathbf{Q}(1+\sqrt{5}).$$

同理，$\mathbf{Q}(\sqrt{2})=\mathbf{Q}(\sqrt{2}-2)$.

由于 $\sqrt[3]{4}=(\sqrt[3]{2})^2$，$\sqrt[3]{2})\in\mathbf{Q}(\sqrt[3]{2})$，$\mathbf{Q}(\sqrt[3]{2})$ 是个域，故

$$\sqrt[3]{4}\in\mathbf{Q}(\sqrt[3]{2}),\quad \mathbf{Q}(\sqrt[3]{4})\subseteq\mathbf{Q}(\sqrt[3]{2}).$$

同时，因为 $\sqrt[3]{2}=\frac{1}{2}(\sqrt[3]{4})^2\in\mathbf{Q}(\sqrt[3]{4})$，知 $\mathbf{Q}(\sqrt[3]{2})\subseteq\mathbf{Q}(\sqrt[3]{4})$. 所以，

$$\mathbf{Q}(\sqrt[3]{2})=\mathbf{Q}(\sqrt[3]{4}).$$

同理,由$\sqrt[4]{2}=\frac{1}{4}(\sqrt[4]{8})^3\in\mathbf{Q}(\sqrt[4]{8})$,知道域

$$\mathbf{Q}(\sqrt[4]{2})=\mathbf{Q}(\sqrt[3]{8}).$$

下面来证明 $\mathbf{Q}(1+\sqrt{3})\neq\mathbf{Q}(\sqrt[4]{3})$. 首先,由于 $\mathbf{Q}(1+\sqrt{3})=\mathbf{Q}(\sqrt{3})$,而$\sqrt{3}$在 $\mathbf{Q}$ 上的极小多项式是 x^2-3,故 $\mathbf{Q}(\sqrt{3})$的元素形如

$$a+b\sqrt{3},\quad a,b\in\mathbf{Q}.$$

如果$\sqrt[4]{3}\in\mathbf{Q}(\sqrt{3})$有 $a,b\in\mathbf{Q}$ 使

$$\sqrt[4]{3}=a+b\sqrt{3},$$

则由 $a+b\sqrt{3}\neq0$,及 $1,\sqrt{3}$在 $\mathbf{Q}$ 上线性无关知 $a\neq0$, $b\neq0$,将两端取平方,得

$$\sqrt[4]{3}=a^2+3b^2-2ab\sqrt[3]{3}.$$

再用 $1,\sqrt{3}$在 $\mathbf{Q}$ 上的线性无关性可推出

$$a^2+3b^2=0,\quad a^2/b^2=-3,\quad a,b\in\mathbf{Q},$$

矛盾. 故 $\mathbf{Q}(\sqrt[4]{3})\neq\mathbf{Q}(\sqrt{3})=\mathbf{Q}(1+\sqrt{3})$.

还可以证明$\sqrt{7}\notin\mathbf{Q}(\sqrt{5})$. 若有 $a,b\in\mathbf{Q}$ 使

$$\sqrt{7}=a+b\sqrt{5},\quad a,b\in\mathbf{Q},\ b\neq0,$$

则有$\sqrt{7}-b\sqrt{5}=a$,两端平方,得

$$7+5b^2-5=2b\sqrt{35}.$$

而 b 不等于 0,此事可推出某有理数之平方为 35,矛盾. 所以,

$$\mathbf{Q}(\sqrt{7})\neq\mathbf{Q}(\sqrt{5}).$$

3. 若 K 为 F 的有限扩张,取 $a_1\in K$, $a_1\notin F$,则 $F(a_1)$是 K 的子域,$F(a_1)$是 F 的有限扩张,且 K 是 $F(a_1)$的有限扩张;再取 $a_2\in K$, $a_2\notin F(a_1)$. 看 $F(a_1,a_2)=F(a_1)(a_2)$, K 又是 $F(a_1,a_2)$的有限扩张…….由于$[K:F]$有限,此事必然有限步终止,得 $K=F(a_1,a_2,\cdots,a_n)$. 每个有限扩张都是代数扩张,a_1,

$a_2,\cdots,a_n$ 当然是F上代数元.

反之,若 $a_1,a_2,\cdots,a_n$ 都是F上的代数元且$K=F(a_1,a_2,\cdots,a_n)$,那么 a_n 当然是$F(a_1,\cdots,a_{n-1})$上的代数元,从而

$$[F(a_1,a_2,\cdots,a_{n-1})(a_n):F(a_1,\cdots,a_{n-1})]$$

有限.同理,a_{n-1}是 $F(a_1,\cdots,a_{n-2})$上的代数元 $F(a_1,\cdots,a_{n-1})$是 $F(a_1,\cdots,a_{n-2})$的有限扩张…….$F(a_1,a_2)$是 $F(a_1)$上有限扩张,$F(a_1)$是 F 上有限扩张,从而

$[F(a_1,a_2,\cdots,a_n):F]=[F(a_1,\cdots,a_{n-1})(a_n):F(a_1,\cdots,a_{n-1})]\times\cdots\times[F(a_1,a_2):F(a_1)]\times[F(a_1):F]$

有限.

4. x^3-6x+6.

5. 由于 $a^2\in F(a)$,故 $F(a^2)\subseteq F(a)$.设 a 在F上的极小多项式的次数为 $2m+1$, 那么

$$2m+1=[F(a):F]=[F(a):F(a^2)][F(a^2):F].$$

因为 a 在$F(a^2)$上满足多项式 x^2-a^2,如果 $a\notin F(a^2)$,那么 a 在$F(a^2)$上的极小多项式必为 2 次,也就是$[F(a):F(a^2)]=2$,进而导出 $2\mid(2m+1)$,矛盾,所以 $a\in F(a^2)$.

6*. 因为 a 是域$F(S)$的代数元,a 必满足一$F(S)$上之多项式

$$f(x)=a_nx^n+\cdots+a_1x+a_0,\quad a_i\in F(S).$$

由于 $F(S)$是 F 上添加 S 生成的域,它的元素 b 均可写成 $h(s_1,\cdots,s_m)/g(s_1,\cdots,s_m)$形式,其中

$$h(x_1,\cdots,x_m),\quad g(x_1,\cdots,x_m)$$

均为 F 上的多项式,而 $s_1,\cdots,s_m$ 可能随b不同而变化,所以,可设

$$a_n=h_n(s_{1n},\cdots,s_{nm})/g_n(s_{1n},\cdots,s_{mn}),$$
$$\cdots,$$
$$a_1=h_1(s_{11},\cdots,s_{m1})/g_1(s_{11},\cdots,s_{m1}),$$
$$a_0=h_0(s_{10},\cdots,s_{m0})/g_0(s_{10},\cdots,s_{m0}).$$

这里本来对每个 a_i 不一定恰好都是 m 个文字多项式 $h_i(x_1, \cdots, x_m)$ 和 $g_i(x_1, \cdots, x_m)$ 来表示之，但多加几个文字不影响表示，例如

$$f(x_1) = x_1^2 + x_1$$

也可写成

$$f(x_1, x_2) = x_1^2 + x_1,$$

这样写起来就整齐了.

现在，令

$$T = \{s_{ij} \mid i = 1, 2, \cdots, m; \; j = 0, \cdots, n\}.$$

则 T 是 S 的 $m(n+1)$ 元子集，且 $f(x)$ 是 $F(T)$ 上的多项式，a 满足 $F(T)$ 上多项式 $f(x)$，a 必为 $F(T)$ 上的代数元.

7*. 在域 $\mathbf{Q}(\sqrt{3}, \mathrm{i})$ 上

$$f(x) = (x - 1 + \sqrt{3})(x - 1 - \sqrt{3})(x + \mathrm{i})(x - \mathrm{i}),$$

即 $f(x)$ 已分解成 $\mathbf{Q}(\sqrt{3}, \mathrm{i})$ 上一次多项式之积.

如还有域 K，使 $\mathbf{Q} \subseteq K \subseteq \mathbf{Q}(\sqrt{3}, \mathrm{i})$，且

$$f(x) = (x - a)(x - b)(x - c)(x - d), \quad a, b, c, d \in K,$$

那么，K 和 $\mathbf{Q}(\sqrt{3}, \mathrm{i})$ 都是复数域 $\mathbf{C}$ 的子域，在 $\mathbf{C}$ 上看，$f(x)$ 有两种分解

$$(x - 1 + \sqrt{3})(x - 1 - \sqrt{3})(x + \mathrm{i})(x - \mathrm{i})$$
$$= (x - a)(x - b)(x - c)(x - d).$$

由于 $\mathbf{C}$ 是唯一分解整数，a, b, c, d 只能是

$$1 - \sqrt{3}, 1 + \sqrt{3}, \mathrm{i}, -\mathrm{i}.$$

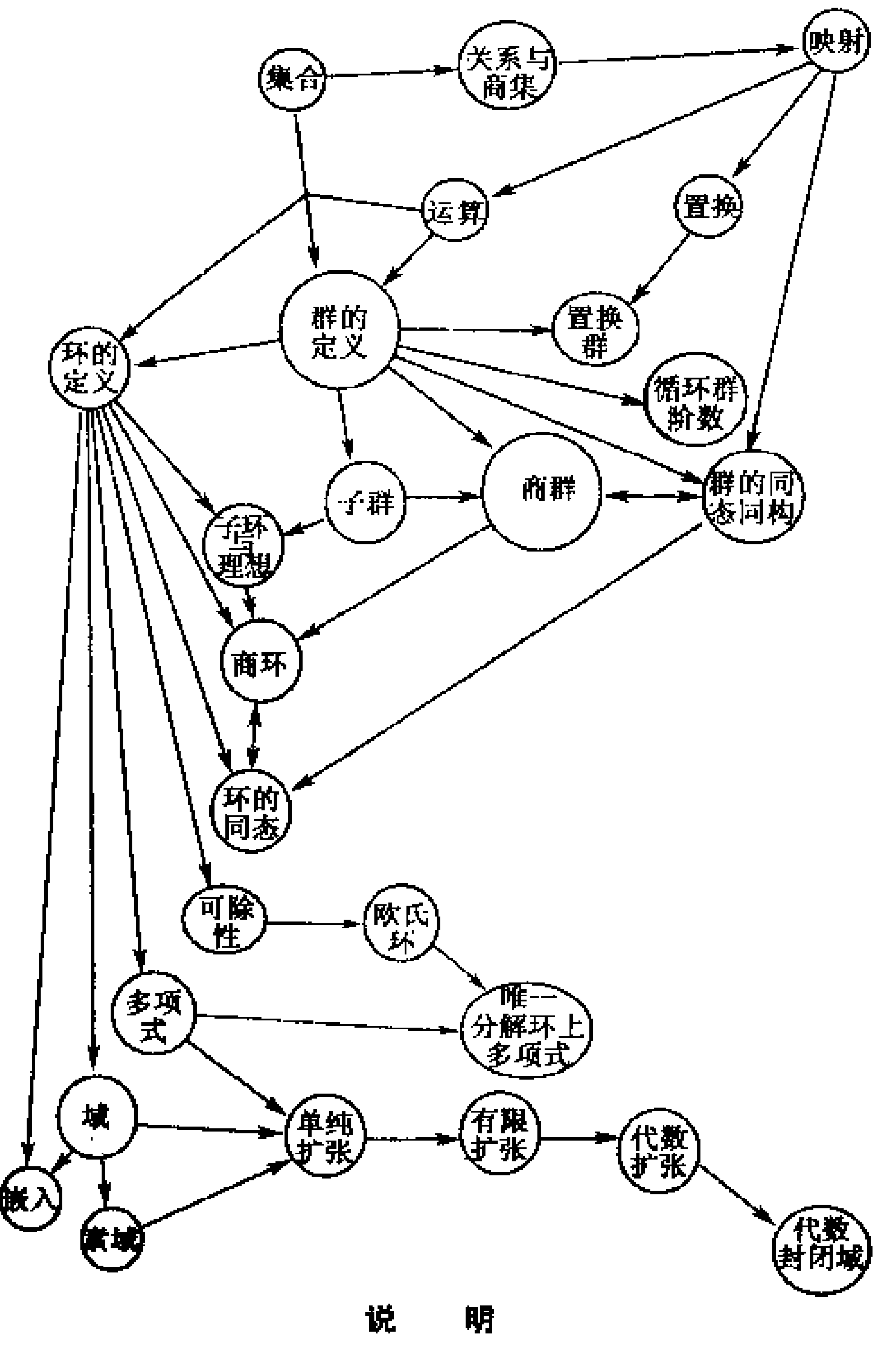
既然 $1 - \sqrt{3}$ 和 $1 + \sqrt{3}$ 都是 K 中，必有 $\sqrt{3} \in K$. 同理 $\mathrm{i} \in K$，$\mathbf{Q}(\sqrt{3}, \mathrm{i}) \subseteq K$.

附录 1　本书中的公理

(1)　有乘法运算·,	(1)′　有加法运算+,
(2)　结合律,	(2)′　结合律,
(3)　有恒等元 1,	(3)′　有恒等元 0(零元),
(4)　每个元均有逆,	(4)′　每个元均有负元,
(5)　交换律	(5)′　交换律
(6)　非空,	
(7)　至少含两个元,	
(8)　有限个元素,	
(9)　分配律,	
(10)　无非零零因子.	

代数系统	**满足公理**
乘法群	(6),(1),(2),(3),(4)
交换群	(6),(1)′,(2)′,(3)′,(4)′,(5)′
有限群	(8),(1),(2),(3),(4)
环	(6),(1)′～(5)′,(1),(2),(9)
交换环	(6),(1)′～(5)′,(1),(2),(9),(5)
有 1 环	(6),(1)′～(5)′,(1),(2),(3),(9)
无零因子环	(6),(1)′～(15)′,(1),(2),(10)
整环	(6),(1)′～(5)′,(1),(2),(3),(9),(5),(10)
除环	(7),(1)′～(5)′,(1),(2),(3),(9),非零元满足(4)
域	(7),(1)′～(5)′,(1),(2),(3),(5),(9),非零元满足(4)

附录 2　各节之间的关系



说　　明

(1) 圆圈分 3 级,越大的越重要;选修内容没列入.

(2) 箭头流向反映概念之间的逻辑关系,不完全依照教材中出现的顺序.

附录3　本书中的重要定理

拉格朗日定理,第二章§5,p.115

设 G 是个有限群.那么 G 的任意子群 H 的阶数一定整除 G 的阶数.

凯莱定理,第三章§2,p.148

每个群 G 都同构于其上所有可逆变换作成的群 $I(G)$ 的一个子群.

第三章§4定理1,p.174

设 N 是群 $(G,\circ)$ 的一个不变子群,G/N 代表 G 对 N 的所有陪集构成的集合.规定,任意 $aN, bN \in G/N$,对应 G/N 的元素 $(a\circ b)N$,则得到 G/N 的一个运算,记为 $\#$,即

$$aN \# bN = (a\circ b)N.$$

进一步,$(G/N, \#)$ 是个群.

群同态基本定理,第三章§4,p.183

设 $(G,\circ)$ 和 $(H,*)$ 都是群,f 是 G 到 H 的满同态映射,$\mathrm{Ker}(f)=K$.那么有映射 $\varphi: G/K \to H$,使得

$$\varphi(aK)=f(a),\quad 对每个\ aK \in G/K,$$

且 φ 是 G/K 到 H 的同构映射.从而

$$G/K \approx H.$$

环同态基本定理,第四章§4,p.261

设 f 是环 $(R,+,\cdot)$ 到环 $(S,\#,\odot)$ 的满的环同态映射,$\mathrm{Ker}(f)=A$.那么 R/A 同构于环 $(S,\#,\odot)$.

第七章§1定理1,p.386

设 F 是个域,$p(x)$ 是 F 上不可约多项式.那么,必有 F 上的一个单纯代数扩张域 $F(\lambda)$ 同构于 $F[x]/(p(x))$,且 $p(x)$ 是 λ 在 F 上的一个极小多项式.

名 词 索 引

一 画

二 画

三 画

四 画

五 画

六　画

七　画

八　画

九　画

十　画

十一　画

十二　画

十三　画

十四画以上

十二 画

十三 画

十四画以上

十二　画

十三　画

十四画以上